* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] This invention relates to the signature document communication device for carrying out exchange of a document and registration of a document to safety in the so-called distributed processing system which aims at improvement in the engine performance or reliability by connecting an information processor or an telecommunications system in a network, and distributing processing among them.
[0002]
[Description of the Prior Art] It is related with the digital signature method in distributed processing, and is Bruce. Schneier work Applied Cryptography Second There are some which were indicated by Edition (WIELY). Drawing 19 is a block diagram showing the component. As for document transmitting-side equipment and 2, in drawing, 1 is [document receiving-side equipment and 4] channels. Document transmitting-side equipment 1 consists of the document editorial department 5 which edits a document, the digital signature generation section 6 which acquires a digital signature from the document after edit, a digital signature adjunct 15 which adds the generated digital signature to a document, and the document transmitting section 16 with a digital signature which transmits a document with a digital signature.
[0003] Moreover, receiving-side equipment 2 consists of the document receive section 18 with a digital signature which receives a document with a digital signature from a channel, the digital signature separation section 17 which separates the received document with a digital signature to a digital signature, and a document, the digital signature verification section 9 which performs alteration of a document, and implementer authentication of a document using a digital signature, and the document editorial department 5 which edits the document after verification.
[0004] Drawing 20 is drawing in which the document with a digital signature generated with document transmitting-side equipment 1 shows the flow transmitted to document receiving-side equipment 2.
[0005] Drawing 21 and drawing 22 are the flow charts which show the flow of processing of document transmitting-side equipment 1 and document receiving-side equipment 2, drawing 21 shows processing with document transmitting-side equipment 1, and drawing 22 shows processing with document receiving-side equipment 2.
[0006] Hereafter, actuation of document transmitting-side equipment 1 is explained, referring to drawing. As shown in drawing 21 , in document transmitting-side equipment 1, the document editorial department 5 generates a document at step S151. Next, the digital signature generation section 6 generates the message digest (henceforth, MD) of a document using a one-way function at step S152 from the generated document. In step S153, a digital signature is generated from generated MD. A digital signature is generated by enciphering using a private key [in / for MD / a document addressee's public key cryptosystem]. The digital signature adjunct 15 is step S154, and the digital signature of a document is added to a document. The document with a digital signature is transmitted to a channel 4 in step S155 by the document transmitting section 16 with a digital signature.

[0007] Next, processing of document receiving-side equipment 2 is explained. As shown in drawing 22 , in document receiving-side equipment 2, the document receive section 18 with a digital signature receives a document with a digital signature at step S161. The received document with a digital signature is separation ******** (step S162) to a digital signature and a document at the digital signature separation section 17. The separated digital signature is decrypted with a transmitting person's public key in a public key cryptosystem in the digital signature verification section 9 (step S163). Regeneration of the MD is carried out from the document furthermore received (step S164). The value of MD which decrypted the digital signature and was obtained in step S163, and MD by which regeneration was carried out at step S164 is compared (step S165). If both are in agreement as a result of a comparison, it will become clear that the transmitting person drew up the document and that the alteration to a creation backward document is not performed (step S166), and when not in agreement, it becomes clear that the alteration to a document was performed (step S167).
[0008]
[Problem(s) to be Solved by the Invention] When the digital signature method currently used for the conventional electronic mail was applied to the file on the file system which OS's, such as UNIX and MS-Windows, treat and a digital signature was added and distributed [saved and] to a file, since the structure of a file changed by adding a digital signature, the application which created the file before a digital signature is added had a trouble of it becoming impossible to process the file to which the digital signature was added.
[0009] This invention was made in order to solve this trouble, and it aims at offering the signature document communication device separated and processed, without making a digital signature add to a file.
[0010] moreover -- although enclosure with big storage capacity is needed when storing and managing the file to which the digital signature was added in the engine proving what the document was drawn up for by him -- a certification engine -- a digital signature -- storing -- a document -- an implementer -- it aims at offering the signature document communication device which cancels the trouble that a certification engine needs mass enclosure that he should just store in his equipment.
[0011]
[Means for Solving the Problem] The signature document communication device concerning invention according to claim 1 is characterized by to have the document transmitting-side equipment which generates a digital signature from this document while generating a document, separates a document and a digital signature, and is transmitted, the document verification information-management equipment which stores while receiving a digital signature, and document receiving-side equipment which verify a document using a digital signature stored in document verification information-management equipment while receiving a document.
[0012] A signature document communication device concerning invention according to claim 2 is characterized by using for document verification information management equipment a hash value of a message digest (henceforth, MD) used for digital signature creation, or MD as an index for searching a digital signature in a signature document communication device according to claim 1.
[0013] In a signature document communication device according to claim 1, document verification information management equipment makes a hash value of MD or MD an index, and a signature document communication device concerning invention according to claim 3 is characterized by including an item which specifies a document as a storing item corresponding to the index in addition to a digital signature.
[0014] A signature document communication device concerning invention according to claim 4 is characterized by document verification information management equipment including an item which pinpoints a storing location of a document as a storing item in addition to a digital signature in a signature document communication device according to claim 3.
[0015] A signature document communication device concerning invention according to claim 5 is characterized by document verification information management equipment including storing positional information of a document which is referring to a document as a storing item in addition to a digital

signature in a signature document communication device according to claim 3.
[0016] A signature document communication device concerning invention according to claim 6 is characterized by document verification information management equipment containing MD of a document which is referring to a document as a storing item corresponding to the index in addition to a digital signature in a signature document communication device according to claim 3.
[0017] A signature document communication device concerning invention according to claim 7 is characterized by document verification information management equipment containing storing positional information and MD of a document which is referring to a document as a storing item corresponding to the index in addition to a digital signature in a signature document communication device according to claim 3.
[0018] A signature document communication device concerning invention according to claim 8 is characterized by document verification information management equipment including key information used for a code and decode processing in addition to said digital signature as a storing item corresponding to the index, and an item stored in the index in a signature document communication device according to claim 3.
[0019] In a signature document communication device according to claim 3, document verification information management equipment makes a hash value of MD an index, and a signature document communication device concerning invention according to claim 9 is characterized by the ability to set up an expiration date to an item stored in the index.
[0020]
[Embodiment of the Invention]
The gestalt 1 of implementation of this invention is explained about drawing below gestalt 1. of operation. Drawing 1 is drawing showing the configuration of the gestalt 1 of operation of this invention, and, for 1, as for document receiving-side equipment and 3, document transmitting-side equipment and 2 are [document verification information management equipment and 4] channels in drawing. Document transmitting-side equipment 1 consists of the document editorial department 5 which edits a document, the digital signature generation section 6 which acquires a digital signature from the document after edit, the digital signature transmitting section 7 which transmits the generated digital signature to document verification information management equipment 3, and the document transmitting section 8 which transmits a document.
[0021] Moreover, document receiving-side equipment 2 consists of the digital signature acquisition section 10 which receives a digital signature from document verification information management equipment 3, a document receive section 11 which receives the document which document transmitting-side equipment 1 transmitted, the digital signature verification section 9 which performs alteration of a document, and implementer authentication of a document using a digital signature, and the document editorial department 5 which edits the document after verification.
[0022] Moreover, document verification information management equipment 3 consists of the digital signature storing processing section 12 for storing the digital signature which received from document transmitting-side equipment and a digital signature storing field 14, and the digital signature retrieval section 13 according to the digital signature retrieval demand from document receiving-side equipment.
[0023] Drawing 2 shows signs that it is transmitted to document receiving-side equipment 2 and the document verification information enclosure 3, respectively, document receiving-side equipment 2 acquires a digital signature from document enclosure, and the document and digital signature which were generated with document transmitting-side equipment 1 verify the received document.
[0024] Drawing 3 and drawing 4 are the flow charts which show processing of document transmitting-side equipment 1 and document receiving-side equipment 2, and drawing 5 is a flow chart in document verification information management equipment 3 which shows the flow of processing.
[0025] Hereafter, actuation in case the document receiving-side equipment 2 which received the document drawn up with document transmitting-side equipment 1 verifies a document is explained, referring to drawing.
[0026] Actuation of the document transmitting-side equipment 1 first shown in the flow chart of

drawing 4 is explained. With document transmitting-side equipment 1, the document editorial department 5 generates a document (step S31). Next, the digital signature generation section 6 generates MD of a document using a one-way function from the generated document (step S32). A digital signature is generated from generated MD (step S33). The digital signature of a document is transmitted to document verification information management equipment 3 with the information used by the digital signature transmitting section 7 as index information at the time of storing (step S34). A document is transmitted to document receiving-side equipment 2 by the document transmitting section 7 (step S35).
[0027] Next, actuation of the document receiving-side equipment 2 shown in the flow chart of drawing 4 is explained. Document receiving-side equipment 2 receives the document which document transmitting-side equipment 2 transmitted in the document receive section 11 (step S41). Next, MD is acquired from the document received in the digital signature verification section 9 (step S42). Next, a digital signature retrieval demand is sent out to document verification information management equipment 3 (step S43). Next, the digital signature acquisition section 10 acquires a digital signature from document verification information management equipment 3 (step S44). The acquired digital signature is decrypted with a transmitting person's public key in a public key cryptosystem in the digital signature verification section 9 (step S45). The value of MD which decrypted the digital signature and was obtained in step S45, and MD by which regeneration was carried out at step S42 is compared (step S46). As a result of a comparison, if both are in agreement, it will become clear that the transmitting person drew up the document and that the alteration to a creation backward document is not performed (step S47), and when not in agreement, it becomes clear that the alteration to a document was performed (step S48).
[0028] Next, actuation of drawing 5 and the document verification information management equipment 3 shown in the flow chart of drawing 6 is explained. Digital signature storing actuation first shown in the flow chart of drawing 5 is explained. If the information containing the digital signature transmitted by step S34 (drawing 3) from document transmitting-side equipment 1 is received (step S51), document verification information management equipment 3 generates index information from the information received with the digital signature, and stores a digital signature (step S52).
[0029] Next, actuation of the response to the digital signature retrieval demand shown in the flow chart of drawing 6 is explained. If digital signature retrieval demand reception is carried out (step S61), document verification information management equipment 3 will search the digital signature which was sent out in step S43 (drawing 4) from document receiving-side equipment 2 and which fills a retrieval demand, and will return it to document receiving-side equipment 2 by considering the digital signature which fills a demand as a response (step S62).
[0030] As mentioned above, alteration verification of that file and implementer authentication can be enabled, enabling processing of the application which created the file to the file on a file system according to the gestalt 1 of this operation. Moreover, it becomes possible to have a guarantee function to the contents of the document by storing and managing only the digital signature of a document also in the documentation-management engine which does not hold mass information enclosure.
[0031] Gestalt 2. drawing 7 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 2 of implementation of this invention, and drawing 8 and drawing 9 are flow charts which show processing. Drawing 8 corresponds to the storing processing (step S34 of drawing 3) to the document verification information management equipment 3 of a digital signature in document transmitting-side equipment 1. Moreover, drawing 9 corresponds to the digital signature storing processing (step S52 of drawing 5) in document verification information management equipment 3.
[0032] In document transmitting-side equipment 1, in case a digital signature is stored in document verification information management equipment 3, the digital signature created from MD and its MD is sent out to document verification information management equipment 3 (step S81). The hash value of MD is calculated (step S92), and document verification information management equipment 3 stores a digital signature in a digital signature storing field by making the calculated hash value into an index, if MD and a digital signature are received (step S91) (step S93). The drawing 7 left part is MD and the

digital signature which are sent out from document transmitting-side equipment 1 in step S81, and the drawing 7 right part expresses MD and the digital signature which were stored in the verification information storing field in step S93.

[0033] As mentioned above, it becomes possible to search a digital signature efficiently by according to the gestalt of this operation, storing in a digital signature storing field by making into an index the hash value of MD which serves as a basis of a digital signature in a digital signature, and storing additionally the information for specifying the digital signature demanded when two or more digital signatures existed to a single index.

[0034] Gestalt 3. drawing 10 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 3 of implementation of this invention. The flow of processing is explained using the flow chart shown in drawing 11 , drawing 12 , drawing 13 , and drawing 14 .

[0035] Drawing 11 corresponds to the storing processing (step S34 of drawing 3) to the document verification information management equipment 3 of a digital signature in document transmitting-side equipment 1. Drawing 12 corresponds to the digital signature storing processing (step S52 of drawing 5) in document verification information management equipment 3. Drawing 13 corresponds to the retrieval demand sending-out processing (step S43 of drawing 4) in document receiving-side equipment 2. Drawing 14 corresponds to the digital signature retrieval demand response processing (drawing 6) in document verification information management equipment 3.

[0036] In document transmitting-side equipment 1, in case a digital signature is stored in document verification information management equipment 3, three items of the digital signature created from MD of MD ** and the creation name of a digital signature are sent out to document verification information management equipment 3 (step S111). The hash value of MD is calculated (step S122), and document verification information management equipment 3 stores **** of a digital signature and a name in a digital signature storing field by making the calculated hash value into an index, if MD, a digital signature, and a name are received (step S121) (step S123). The drawing 10 left parts are MD sent out from document transmitting-side equipment 1 in step S111, a digital signature, and a name, and the drawing 10 right part expresses MD stored in the verification information storing field in step S123, the digital signature, and the name.

[0037] In step S43, document receiving-side equipment 2 includes the author of MD calculated at step S43, and the received document in a digital signature retrieval demand, and sends him out to document verification information management equipment 3 (step S131). The document verification information management equipment 3 which received the digital signature retrieval demand calculates the hash value of MD contained in a retrieval demand (step S141). Next, it investigates whether **** containing the author name of the digital signature of the digital signature which makes an index the calculated hash value, and a name which constructs and is contained in a retrieval demand in inside exists (step S142). When it exists, it answers document receiving-side equipment 2 by considering only the corresponding group Mika digital signatures of the author name of a digital signature and a digital signature as a retrieval demand response (step S143). When it does not exist, it answers document receiving-side equipment by considering NULL as a retrieval demand response (step S144).

[0038] Gestalt 4. drawing 15 of operation is drawing showing the contents of the verification information storing field of the document verification information-management equipment in the gestalt 4 of implementation of this invention, sends out the MD and the document location where document transmitting-side equipment 1 serves as the basis of a digital signature at a digital-signature storing demand with a digital signature, and shows signs that the document verification information-management equipment 3 which received them stores a digital signature and a document location in a digital-signature storing field 14 by making the hash value of MD into an index.

[0039] As mentioned above, since the positional information of a document was added to the storing item according to the gestalt of this operation, document transmitting-side equipment 1 does not send the substance of a document to document receiving-side equipment 2, but it is only that ** also sends MD, and document receiving-side equipment 2 can acquire the document which document transmitting-

side equipment 1 drew up based on that MD, and it can lessen information sent to document receiving-side equipment 2 from document transmitting-side equipment 1.
[0040] Gestalt 5. drawing 16 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 5 of implementation of this invention. MD from which document transmitting-side equipment 1 becomes a digital signature storing demand with the basis of a digital signature, MD of the document which the drawn-up document refers to is sent out with a digital signature, and signs that MD of the document which the document verification information management equipment 3 which received them referred to with the digital signature by making the hash value of MD into an index to the digital signature storing field 14 is stored are shown. Signs that the document whose MD is MD1 is specifically referring to the document whose MD is MD3 are shown.
[0041] As mentioned above, since MD of the document which the document is referring to was added to the storing item according to the gestalt of this operation, a document and the document currently referred to can be connected.
[0042] Gestalt 6. drawing 17 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 6 of implementation of this invention. MD from which document transmitting-side equipment 1 becomes a digital signature storing demand with the basis of a digital signature, The document location of the document which MD of the document which the drawn-up document refers to, and the drawn-up document refer to is sent out with a digital signature. MD of the document which the document verification information management equipment 3 which received them referred to with the digital signature by making the hash value of MD into an index to the digital signature storing field 14, and signs that a document location is stored are shown. Specifically, the document location whose MD the document whose MD is MD1 is MD3 shows signs that the document of the document location 3 is referred to.
[0043] As mentioned above, since MD of the document which the document is referring to, and the positional information of the document which the document is referring to were added to the storing item according to the gestalt of this operation, document receiving-side equipment 2 can acquire and verify the document which not only the verification of a document that received but the received document is referring to.
[0044] Gestalt 7. drawing 18 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 7 of implementation of this invention. MD from which document transmitting-side equipment 1 becomes a digital signature storing demand with the basis of a digital signature, The key used for a decryption in case the document is enciphered is sent out with a digital signature, and signs that the document verification information management equipment 3 which received them stores a digital signature and a key in the digital signature storing field 14 by making the hash value of MD into an index are shown. Signs that the key 1 specifically used for a decryption of the enciphered document whose MD is MD1 is stored in the digital signature storing field 14 are shown.
[0045] As mentioned above, since the key information used for a decryption of the document enciphered was added to the storing item according to the gestalt of this operation, encryption of the document which can decrypt only within an expiration date is attained by preparing an expiration date, for example in a storing item.
[0046]
[Effect of the Invention] The signature document communication device concerning invention according to claim 1 While receiving the document transmitting-side equipment which generates a digital signature from this document while generating a document, separates a document and a digital signature, and is transmitted, and a digital signature Since it was made the configuration equipped with the document verification information management equipment to store and the document receiving-side equipment which verifies a document using the digital signature stored in document verification information management equipment while receiving a document Alteration verification of the file and implementer

authentication can be enabled, enabling processing of the application which created the file to the file on a file system. Moreover, it becomes possible to have a guarantee function to the contents of the document by storing and managing only the digital signature of a document also in the documentation-management engine which does not hold mass information enclosure.

[0047] Since the hash value of the message digest (henceforth, MD) by which the signature document communication device concerning invention according to claim 2 was used for digital signature creation as an index for document verification information management equipment to search a digital signature, or MD is used, it becomes possible to search a digital signature efficiently.

[0048] Since document verification information management equipment includes the item which makes the hash value of MD or MD an index, and specifies a document as a storing item corresponding to the index in addition to a digital signature, the signature document communication device concerning invention according to claim 3 becomes possible [searching a digital signature efficiently].

[0049] Since document verification information management equipment includes the item which pinpoints the storing location of a document as a storing item in addition to a digital signature, the signature document communication device concerning invention according to claim 4 can connect a document and the document currently referred to.

[0050] Since document verification information management equipment includes the storing positional information of the document which is referring to the document as a storing item in addition to a digital signature, the signature document communication device concerning invention according to claim 5 can lessen information sent to document receiving-side equipment from document transmitting-side equipment.

[0051] Since document verification information management equipment contains MD of a document which is referring to the document as a storing item corresponding to the index in addition to a digital signature, the signature document communication device concerning invention according to claim 6 can connect a document and the document currently referred to.

[0052] Since the signature document communication device concerning invention according to claim 7 contains the storing positional information and MD of a document which are referring to the document as a storing item corresponding to the index in addition to a digital signature, document receiving-side equipment can acquire and verify the document which not only the verification of a document that received but the received document is referring to.

[0053] Since the signature document communication device concerning invention according to claim 8 includes the key information used for a code and decode processing in addition to a digital signature as the storing item corresponding to the index, and an item stored in the index, it can store key information required for a decryption of the enciphered document which is verified by the digital signature in document verification information management equipment.

[0054] Document verification information management equipment makes the hash value of MD an index, and since the signature document communication device concerning invention according to claim 9 can set up an expiration date to the item stored in the index, the encryption of the document which can decrypt only within an expiration date of it is attained.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] The signature document communication device concerning invention according to claim 1, While receiving the document transmitting-side equipment which generates a digital signature from this document while generating a document, separates a document and a digital signature, and is transmitted, and a digital signature Since it was made the configuration equipped with the document verification information management equipment to store and the document receiving-side equipment which verifies a document using the digital signature stored in document verification information management equipment while receiving a document Alteration verification of the file and implementer authentication can be enabled, enabling processing of the application which created the file to the file on a file system. Moreover, it becomes possible to have a guarantee function to the contents of the document by storing and managing only the digital signature of a document also in the documentation-management engine which does not hold mass information enclosure.
[0047] Since the hash value of the message digest (henceforth, MD) by which the signature document communication device concerning invention according to claim 2 was used for digital signature creation as an index for document verification information management equipment to search a digital signature, or MD is used, it becomes possible to search a digital signature efficiently.
[0048] Since document verification information management equipment includes the item which makes the hash value of MD or MD an index, and specifies a document as a storing item corresponding to the index in addition to a digital signature, the signature document communication device concerning invention according to claim 3 becomes possible [searching a digital signature efficiently].
[0049] Since document verification information management equipment includes the item which pinpoints the storing location of a document as a storing item in addition to a digital signature, the signature document communication device concerning invention according to claim 4 can connect a document and the document currently referred to.
[0050] Since document verification information management equipment includes the storing positional information of the document which is referring to the document as a storing item in addition to a digital signature, the signature document communication device concerning invention according to claim 5 can lessen information sent to document receiving-side equipment from document transmitting-side equipment.
[0051] Since document verification information management equipment contains MD of a document which is referring to the document as a storing item corresponding to the index in addition to a digital signature, the signature document communication device concerning invention according to claim 6 can connect a document and the document currently referred to.
[0052] Since the signature document communication device concerning invention according to claim 7 contains the storing positional information and MD of a document which are referring to the document as a storing item corresponding to the index in addition to a digital signature, document receiving-side equipment can acquire and verify the document which not only the verification of a document that received but the received document is referring to.
[0053] Since the signature document communication device concerning invention according to claim 8

includes the key information used for a code and decode processing in addition to a digital signature as the storing item corresponding to the index, and an item stored in the index, it can store key information required for a decryption of the enciphered document which is verified by the digital signature in document verification information management equipment.
[0054] Document verification information management equipment makes the hash value of MD an index, and since the signature document communication device concerning invention according to claim 9 can set up an expiration date to the item stored in the index, the encryption of the document which can decrypt only within an expiration date of it is attained.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] When the digital signature method currently used for the conventional electronic mail was applied to the file on the file system which OS's, such as UNIX and MS-Windows, treat and a digital signature was added and distributed [saved and] to a file, since the structure of a file changed by adding a digital signature, the application which created the file before a digital signature is added had a trouble of it becoming impossible to process the file to which the digital signature was added.
[0009] This invention was made in order to solve this trouble, and it aims at offering the signature document communication device separated and processed, without making a digital signature add to a file.
[0010] moreover -- although enclosure with big storage capacity is needed when storing and managing the file to which the digital signature was added in the engine proving what the document was drawn up for by him -- a certification engine -- a digital signature -- storing -- a document -- an implementer -- it aims at offering the signature document communication device which cancels the trouble that a certification engine needs mass enclosure that he should just store in his equipment.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] The signature document communication device concerning invention according to claim 1 is characterized by to have the document transmitting-side equipment which generates a digital signature from this document while generating a document, separates a document and a digital signature, and is transmitted, the document verification information-management equipment which stores while receiving a digital signature, and document receiving-side equipment which verify a document using a digital signature stored in document verification information-management equipment while receiving a document.
[0012] A signature document communication device concerning invention according to claim 2 is characterized by using for document verification information management equipment a hash value of a message digest (henceforth, MD) used for digital signature creation, or MD as an index for searching a digital signature in a signature document communication device according to claim 1.
[0013] In a signature document communication device according to claim 1, document verification information management equipment makes a hash value of MD or MD an index, and a signature document communication device concerning invention according to claim 3 is characterized by including an item which specifies a document as a storing item corresponding to the index in addition to a digital signature.
[0014] A signature document communication device concerning invention according to claim 4 is characterized by document verification information management equipment including an item which pinpoints a storing location of a document as a storing item in addition to a digital signature in a signature document communication device according to claim 3.
[0015] A signature document communication device concerning invention according to claim 5 is characterized by document verification information management equipment including storing positional information of a document which is referring to a document as a storing item in addition to a digital signature in a signature document communication device according to claim 3.
[0016] A signature document communication device concerning invention according to claim 6 is characterized by document verification information management equipment containing MD of a document which is referring to a document as a storing item corresponding to the index in addition to a digital signature in a signature document communication device according to claim 3.
[0017] A signature document communication device concerning invention according to claim 7 is characterized by document verification information management equipment containing storing positional information and MD of a document which is referring to a document as a storing item corresponding to the index in addition to a digital signature in a signature document communication device according to claim 3.
[0018] A signature document communication device concerning invention according to claim 8 is characterized by document verification information management equipment including key information used for a code and decode processing in addition to said digital signature as a storing item corresponding to the index, and an item stored in the index in a signature document communication device according to claim 3.

[0019] In a signature document communication device according to claim 3, document verification information management equipment makes a hash value of MD an index, and a signature document communication device concerning invention according to claim 9 is characterized by the ability to set up an expiration date to an item stored in the index.
[0020]
[Embodiment of the Invention]
The gestalt 1 of implementation of this invention is explained about drawing below gestalt 1. of operation. Drawing 1 is drawing showing the configuration of the gestalt 1 of operation of this invention, and, for 1, as for document receiving-side equipment and 3, document transmitting-side equipment and 2 are [document verification information management equipment and 4] channels in drawing. Document transmitting-side equipment 1 consists of the document editorial department 5 which edits a document, the digital signature generation section 6 which acquires a digital signature from the document after edit, the digital signature transmitting section 7 which transmits the generated digital signature to document verification information management equipment 3, and the document transmitting section 8 which transmits a document.
[0021] Moreover, document receiving-side equipment 2 consists of the digital signature acquisition section 10 which receives a digital signature from document verification information management equipment 3, a document receive section 11 which receives the document which document transmitting-side equipment 1 transmitted, the digital signature verification section 9 which performs alteration of a document, and implementer authentication of a document using a digital signature, and the document editorial department 5 which edits the document after verification.
[0022] Moreover, document verification information management equipment 3 consists of the digital signature storing processing section 12 for storing the digital signature which received from document transmitting-side equipment and a digital signature storing field 14, and the digital signature retrieval section 13 according to the digital signature retrieval demand from document receiving-side equipment.
[0023] Drawing 2 shows signs that it is transmitted to document receiving-side equipment 2 and the document verification information enclosure 3, respectively, document receiving-side equipment 2 acquires a digital signature from document enclosure, and the document and digital signature which were generated with document transmitting-side equipment 1 verify the received document.
[0024] Drawing 3 and drawing 4 are the flow charts which show processing of document transmitting-side equipment 1 and document receiving-side equipment 2, and drawing 5 is a flow chart in document verification information management equipment 3 which shows the flow of processing.
[0025] Hereafter, actuation in case the document receiving-side equipment 2 which received the document drawn up with document transmitting-side equipment 1 verifies a document is explained, referring to drawing.
[0026] Actuation of the document transmitting-side equipment 1 first shown in the flow chart of drawing 4 is explained. With document transmitting-side equipment 1, the document editorial department 5 generates a document (step S31). Next, the digital signature generation section 6 generates MD of a document using a one-way function from the generated document (step S32). A digital signature is generated from generated MD (step S33). The digital signature of a document is transmitted to document verification information management equipment 3 with the information used by the digital signature transmitting section 7 as index information at the time of storing (step S34). A document is transmitted to document receiving-side equipment 2 by the document transmitting section 7 (step S35).
[0027] Next, actuation of the document receiving-side equipment 2 shown in the flow chart of drawing 4 is explained. Document receiving-side equipment 2 receives the document which document transmitting-side equipment 2 transmitted in the document receive section 11 (step S41). Next, MD is acquired from the document received in the digital signature verification section 9 (step S42). Next, a digital signature retrieval demand is sent out to document verification information management equipment 3 (step S43). Next, the digital signature acquisition section 10 acquires a digital signature from document verification information management equipment 3 (step S44). The acquired digital signature is decrypted with a transmitting person's public key in a public key cryptosystem in the digital

signature verification section 9 (step S45). The value of MD which decrypted the digital signature and was obtained in step S45, and MD by which regeneration was carried out at step S42 is compared (step S46). As a result of a comparison, if both are in agreement, it will become clear that the transmitting person drew up the document and that the alteration to a creation backward document is not performed (step S47), and when not in agreement, it becomes clear that the alteration to a document was performed (step S48).

[0028] Next, actuation of drawing 5 and the document verification information management equipment 3 shown in the flow chart of drawing 6 is explained. Digital signature storing actuation first shown in the flow chart of drawing 5 is explained. If the information containing the digital signature transmitted by step S34 (drawing 3) from document transmitting-side equipment 1 is received (step S51), document verification information management equipment 3 generates index information from the information received with the digital signature, and stores a digital signature (step S52).

[0029] Next, actuation of the response to the digital signature retrieval demand shown in the flow chart of drawing 6 is explained. If digital signature retrieval demand reception is carried out (step S61), document verification information management equipment 3 will search the digital signature which was sent out in step S43 (drawing 4) from document receiving-side equipment 2 and which fills a retrieval demand, and will return it to document receiving-side equipment 2 by considering the digital signature which fills a demand as a response (step S62).

[0030] As mentioned above, alteration verification of that file and implementer authentication can be enabled, enabling processing of the application which created the file to the file on a file system according to the gestalt 1 of this operation. Moreover, it becomes possible to have a guarantee function to the contents of the document by storing and managing only the digital signature of a document also in the documentation-management engine which does not hold mass information enclosure.

[0031] Gestalt 2. drawing 7 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 2 of implementation of this invention, and drawing 8 and drawing 9 are flow charts which show processing. Drawing 8 corresponds to the storing processing (step S34 of drawing 3) to the document verification information management equipment 3 of a digital signature in document transmitting-side equipment 1. Moreover, drawing 9 corresponds to the digital signature storing processing (step S52 of drawing 5) in document verification information management equipment 3.

[0032] In document transmitting-side equipment 1, in case a digital signature is stored in document verification information management equipment 3, the digital signature created from MD and its MD is sent out to document verification information management equipment 3 (step S81). The hash value of MD is calculated (step S92), and document verification information management equipment 3 stores a digital signature in a digital signature storing field by making the calculated hash value into an index, if MD and a digital signature are received (step S91) (step S93). The drawing 7 left part is MD and the digital signature which are sent out from document transmitting-side equipment 1 in step S81, and the drawing 7 right part expresses MD and the digital signature which were stored in the verification information storing field in step S93.

[0033] As mentioned above, it becomes possible to search a digital signature efficiently by according to the gestalt of this operation, storing in a digital signature storing field by making into an index the hash value of MD which serves as a basis of a digital signature in a digital signature, and storing additionally the information for specifying the digital signature demanded when two or more digital signatures existed to a single index.

[0034] Gestalt 3. drawing 10 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 3 of implementation of this invention. The flow of processing is explained using the flow chart shown in drawing 11 , drawing 12 , drawing 13 , and drawing 14 .

[0035] Drawing 11 corresponds to the storing processing (step S34 of drawing 3) to the document verification information management equipment 3 of a digital signature in document transmitting-side equipment 1. Drawing 12 corresponds to the digital signature storing processing (step S52 of drawing

5) in document verification information management equipment 3. Drawing 13 corresponds to the retrieval demand sending-out processing (step S43 of drawing 4) in document receiving-side equipment 2. Drawing 14 corresponds to the digital signature retrieval demand response processing (drawing 6) in document verification information management equipment 3.

[0036] In document transmitting-side equipment 1, in case a digital signature is stored in document verification information management equipment 3, three items of the digital signature created from MD of MD ** and the creation name of a digital signature are sent out to document verification information management equipment 3 (step S111). The hash value of MD is calculated (step S122), and document verification information management equipment 3 stores **** of a digital signature and a name in a digital signature storing field by making the calculated hash value into an index, if MD, a digital signature, and a name are received (step S121) (step S123). The drawing 10 left parts are MD sent out from document transmitting-side equipment 1 in step S111, a digital signature, and a name, and the drawing 10 right part expresses MD stored in the verification information storing field in step S123, the digital signature, and the name.

[0037] In step S43, document receiving-side equipment 2 includes the author of MD calculated at step S43, and the received document in a digital signature retrieval demand, and sends him out to document verification information management equipment 3 (step S131). The document verification information management equipment 3 which received the digital signature retrieval demand calculates the hash value of MD contained in a retrieval demand (step S141). Next, it investigates whether **** containing the author name of the digital signature of the digital signature which makes an index the calculated hash value, and a name which constructs and is contained in a retrieval demand in inside exists (step S142). When it exists, it answers document receiving-side equipment 2 by considering only the corresponding group Mika digital signatures of the author name of a digital signature and a digital signature as a retrieval demand response (step S143). When it does not exist, it answers document receiving-side equipment by considering NULL as a retrieval demand response (step S144).

[0038] Gestalt 4. drawing 15 of operation is drawing showing the contents of the verification information storing field of the document verification information-management equipment in the gestalt 4 of implementation of this invention, sends out the MD and the document location where document transmitting-side equipment 1 serves as the basis of a digital signature at a digital-signature storing demand with a digital signature, and shows signs that the document verification information-management equipment 3 which received them stores a digital signature and a document location in a digital-signature storing field 14 by making the hash value of MD into an index.

[0039] As mentioned above, since the positional information of a document was added to the storing item according to the gestalt of this operation, document transmitting-side equipment 1 does not send the substance of a document to document receiving-side equipment 2, but it is only that ** also sends MD, and document receiving-side equipment 2 can acquire the document which document transmitting-side equipment 1 drew up based on that MD, and it can lessen information sent to document receiving-side equipment 2 from document transmitting-side equipment 1.

[0040] Gestalt 5. drawing 16 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 5 of implementation of this invention. MD from which document transmitting-side equipment 1 becomes a digital signature storing demand with the basis of a digital signature, MD of the document which the drawn-up document refers to is sent out with a digital signature, and signs that MD of the document which the document verification information management equipment 3 which received them referred to with the digital signature by making the hash value of MD into an index to the digital signature storing field 14 is stored are shown. Signs that the document whose MD is MD1 is specifically referring to the document whose MD is MD3 are shown.

[0041] As mentioned above, since MD of the document which the document is referring to was added to the storing item according to the gestalt of this operation, a document and the document currently referred to can be connected.

[0042] Gestalt 6. drawing 17 of operation is drawing showing the contents of the verification

information storing field of the document verification information management equipment in the gestalt 6 of implementation of this invention. MD from which document transmitting-side equipment 1 becomes a digital signature storing demand with the basis of a digital signature, The document location of the document which MD of the document which the drawn-up document refers to, and the drawn-up document refer to is sent out with a digital signature. MD of the document which the document verification information management equipment 3 which received them referred to with the digital signature by making the hash value of MD into an index to the digital signature storing field 14, and signs that a document location is stored are shown. Specifically, the document location whose MD the document whose MD is MD1 is MD3 shows signs that the document of the document location 3 is referred to.

[0043] As mentioned above, since MD of the document which the document is referring to, and the positional information of the document which the document is referring to were added to the storing item according to the gestalt of this operation, document receiving-side equipment 2 can acquire and verify the document which not only the verification of a document that received but the received document is referring to.

[0044] Gestalt 7. drawing 18 of operation is drawing showing the contents of the verification information storing field of the document verification information management equipment in the gestalt 7 of implementation of this invention. MD from which document transmitting-side equipment 1 becomes a digital signature storing demand with the basis of a digital signature, The key used for a decryption in case the document is enciphered is sent out with a digital signature, and signs that the document verification information management equipment 3 which received them stores a digital signature and a key in the digital signature storing field 14 by making the hash value of MD into an index are shown. Signs that the key 1 specifically used for a decryption of the enciphered document whose MD is MD1 is stored in the digital signature storing field 14 are shown.

[0045] As mentioned above, since the key information used for a decryption of the document enciphered was added to the storing item according to the gestalt of this operation, encryption of the document which can decrypt only within an expiration date is attained by preparing an expiration date, for example in a storing item.

[Translation done.]

File 347:JAPIO Oct 1976-2003/Oct(Updated 040202)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200410
(c) 2004 Thomson Derwent

Set	Items	Description
S1	21096	SIGNATURE? ? OR HASH?? OR DIGEST? ?
S2	7925	CYCLIC?()REDUNDAN??()(CHECK? OR COD???) OR CRC OR FRAME()CHECK()SEQUENCE? ? OR FCS OR CHECKSUM? ? OR CHECKDIGIT? ? OR CHECKBIT? ? OR CHECK()(SUM? ? OR DIGIT? ? OR BIT? ?) OR BCC OR BLOCK()CHECK()CHARACTER? ? OR CONTROL()DIGIT? ?
S3	4405	(PARITY OR REDUNDANT)(1W)(CODEWORD? ? OR CODE OR BLOCK? ? OR CODEBLOCK? ? OR BIT? ?) OR SYNDROME(1W)BIT? ?
S4	1945384	SEPARATE OR SEPARATELY OR INDEPENDENT OR DETACHED OR UNATTACHED OR (DE OR UN)()ATTACHED OR DISCONNECTED OR ISOLATED OR APART()"FROM"
S5	1902642	WITHOUT OR BY()ITSELF OR ("NOT" OR T)(1W)(INCLUD? OR ATTACH? OR WITH OR CONNECT? OR DEPENDENT?)
S6	214	S1:S3(5N)S4:S5(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSION OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BROADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COMMUNICAT? OR FORWARD?)
S7	100	S1 AND S6
S8	19	S7 AND IC=G09C
S9	81	S7 NOT S8
S10	15	S9 AND IC=H04L
S11	66	S9 NOT S10
S12	14	S11 AND IC=G06F
S13	52	S11 NOT S12
S14	0	S1(5N)IDEPENDENTLY(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSION OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BROADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COMMUNICAT? OR FORWARD?)

8/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

06941351 **Image available**
MAIL SERVER

PUB. NO.: 2001-168902 [JP 2001168902 A]
PUBLISHED: June 22, 2001 (20010622)
INVENTOR(s): NAKATSUCHI SHOJI
YAMAMOTO MASAAKI
APPLICANT(s): NTT DOCOMO INC
APPL. NO.: 11-350404 [JP 99350404]
FILED: December 09, 1999 (19991209)
INTL CLASS: H04L-012/54; H04L-012/58; G06F-013/00; **G09C-001/00** ; H04L-009/32

ABSTRACT

PROBLEM TO BE SOLVED: To provide a mail server that can **transmit** an electronic mail with a digital **signature** to a destination, **without** increasing traffic of a data **transmission** channel and has a security effect of the digital **signature** , even when a mail transmitter terminal has no configuration for the digital **signature** .

SOLUTION: A gateway server 22 contained in a mobile packet communication network 20 which is a closed network receives electronic mails from mobile stations 10A, 10B, etc., and applies a digital **signature** to the received electronic mails. Then the gateway server 22 transmits the electronic mails with the digital **signature** applied to them to a personal computer 40A through the Internet 30. The personal computer 40A analyzes the received electronic mails and the digital **signature** to detect the existence of forgery.

COPYRIGHT: (C)2001,JPO

8/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

06914861 **Image available**
DIGITAL **SIGNATURE** METHOD, METHOD AND SYSTEM FOR MANAGING SECRET INFORMATION

PUB. NO.: 2001-142397 [JP 2001142397 A]
PUBLISHED: May 25, 2001 (20010525)
INVENTOR(s): MIYAZAKI KUNIHIKO
TAKARAGI KAZUO
APPLICANT(s): HITACHI LTD
APPL. NO.: 11-307993 [JP 99307993]
FILED: October 29, 1999 (19991029)
PRIORITY: 10-309936 [JP 98309936], JP (Japan), October 30, 1998 (19981030)
11-241905 [JP 99241905], JP (Japan), August 27, 1999 (19990827)
INTL CLASS: **G09C-001/00** ; G06F-012/14

ABSTRACT

PROBLEM TO BE SOLVED: To provide digital **signature** with high processing efficiency and the distribution control technique of a key.
SOLUTION: The computer 1002 of a card holder and an IC card A or B generate a **signature** cooperatively **without distributing** the secrecy of random numbers generated by each of them. Further, data used for generating the **signature** are used for ciphering as a key.

COPYRIGHT: (C)2001,JPO

8/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

06466660 **Image available**
PRIVACY DISTRIBUTED SYSTEM AND RECORDING MEDIUM

PUB. NO.: 2001-034164 [JP 2001034164 A]
PUBLISHED: February 09, 2001 (20010209)
INVENTOR(s): SAKURAI KOICHI
MIYAZAKI SHINGO
APPLICANT(s): TOSHIBA CORP
APPL. NO.: 11-209891 [JP 99209891]
FILED: July 23, 1999 (19990723)
INTL CLASS: **G09C-001/00** ; G06F-012/14; H04L-009/08; H04L-009/10

ABSTRACT

PROBLEM TO BE SOLVED: To realize a **distributed** decoding and **signature** by arbitrary (t) agencies among (n) agencies **without** calculating secret keys at environments where distributors are not present.

SOLUTION: In this privacy distributed system, (n) respective agencies P1 to Pn preserve one of partial information di (0≤i≤n) of an (n, n) type and the partial information di are made to be t(r+1) of partial random numbers Sj of a (t, n) type and these (r+1) pieces of partial random numbers Sj are distributed to respective agencies P1 to Pn based on t-ary displays (tj-th value k, 0≤k≤t-1, 0≤i≤r) of identification numbers (z) of the respective agencies P1 to Pn and (r+1) of partial information dj, k are obtained by collecting partial random numbers distributed each other for every figure tj of the t-ary displays. Next, a user device U transmits ciphered data C by selecting (t) of agencies Tz and (t) of agencies Tz answer partial outputs Xz which are obtained by them by arithmetically processing the chipherd data C based on the partial information di, k respectively to the user device U then, the device U composes the (t) of partial outputs Xz to obtain a decoded result.

COPYRIGHT: (C)2001,JPO

8/5/4 (Item 4 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

06516108 **Image available**
DIGITAL VIDEO CODING/DECODING DEVICE USING WATERMARKING TO RECORD AND DECODE **SIGNATURE** VIDEO IMAGE AND ITS METHOD

PUB. NO.: 2000-101826 [JP 2000101826 A]
PUBLISHED: April 07, 2000 (20000407)
INVENTOR(s): SHIN GENDO
APPLICANT(s): SAMSUNG ELECTRONICS CO LTD
APPL. NO.: 11-186591 [JP 99186591]
FILED: June 30, 1999 (19990630)
PRIORITY: 91542 [US 9891542], US (United States of America), July 01, 1998 (19980701)
INTL CLASS: H04N-001/387; G06T-001/00; **G09C-005/00** ; H04N-007/30

ABSTRACT

PROBLEM TO BE SOLVED: To allow the device to record and decode a **signature** video image by using water marking **without** increase a quantity of **transfer** data and the need of providing an original host video image.

SOLUTION: The digital video coding device is provided with a 1st discrete wavelet transform section 202 that applies discrete wavelet transform to a host video image and provides an output of M×M wavelet coefficients, a 2nd discrete wavelet transform section 204 that applies discrete wavelet transform to a **signature** video image and provides an output of N×N (N is equal to or less than M) wavelet coefficients, a pseudo random number

generating section 206 that receives an encryption code and generates a pseudo random number according to prescribed rules, and a coefficient replacement section 208 that sets N×N sets of replacement positions, replaces coefficients at N×N positions among the M×M discrete wavelet coefficients with the N×N wavelet coefficients and outputs the replaced M×M wavelet coefficients.

8/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

06261187 **Image available**
DIGITAL **SIGNATURE** SYSTEM, AND COMMUNICATION EQUIPMENT AND INFORMATION COMMUNICATION SYSTEM USING THE SAME

PUB. NO.: 11-202767 [JP 11202767 A]
PUBLISHED: July 30, 1999 (19990730)
INVENTOR(s): OISHI KAZUOMI
APPLICANT(s): CANON INC
APPL. NO.: 10-006630 [JP 986630]
FILED: January 16, 1998 (19980116)
INTL CLASS: **G09C-001/00** ; H04L-009/32

ABSTRACT

PROBLEM TO BE SOLVED: To provide an information **communication** system for surely keeping the anonymity of a group **signature** **without** the need of the exchange of member and authority.

SOLUTION: A means 20 uses the public information v of a user (j) instead of a public parameter PV, generates a digital **signature** (m, r, s) with respect to digital information (m) and secretly transmits it to the user (j). The means 36 obtains a different value by converting the digital **signature** (m, r, s) by using secret information sj of the user (j), considers a value obtained from the digital information (m), the digital **signature** (m, r, s) and the public information of a signing person as the public information, considers the value for which the digital **signature** (m, r, s) is converted, as the secret information of the user (j) and thus, generates the digital **signature** (m, r, m', r', s').

8/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

05697054 **Image available**
SIGNATURED DOCUMENT COMMUNICATION DEVICE

PUB. NO.: 09-311854 [JP 9311854 A]
PUBLISHED: December 02, 1997 (19971202)
INVENTOR(s): YONEDA TAKESHI
APPLICANT(s): MITSUBISHI ELECTRIC CORP [000601] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-127360 [JP 96127360]
FILED: May 22, 1996 (19960522)
INTL CLASS: [6] G06F-017/21; G06F-012/00; G06F-012/00; **G09C-001/00** ; H04L-009/32
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION PROCESSING -- Memory Units)

ABSTRACT

PROBLEM TO BE SOLVED: To separately process a digital **signature** without adding to to a file by receiving a document and also verifying the document

by using the digital **signature** .
SOLUTION: This device includes a document **transmitting** device 1 which generates a document, generates a digital **signature** from the document and **transmits** the document and the digital **signature** **separate** from each other, a document verification information management device 3 which receives and stores the digital **signature** , and a document receiving device 2 which receives the document and verifies the document by means of the digital **signature** stored in the device 3. In such a constitution, the application that produced a file of a file system can be processed and also it is possible to verify the alteration of the file and to authenticate the producer of the file. In addition, even a document management organ that has no information storage device of large capacity can have an assurance function by storing and managing only the digital **signature** of a document.

8/5/7 (Item 7 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

05393999 **Image available**
METHOD AND SYSTEM FOR DATA COMMUNICATION

PUB. NO.: 09-008799 [JP 9008799 A]
PUBLISHED: January 10, 1997 (19970110)
INVENTOR(s): AOYAMA YUUGO
IWAMA MITSUO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 07-158134 [JP 95158134]
FILED: June 23, 1995 (19950623)
INTL CLASS: [6] H04L-009/32; G06F-013/00; **G09C-001/00** ; H04L-009/08
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems); 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION PROCESSING -- Memory Units)

ABSTRACT

PURPOSE: To check the error of a communication sentence and whether the **communication** sentence comes from regular **communication** equipment or not **without** lowering **communication** performance by setting a **signature** generated by a **transmitter** as seal information and sending it when transmitting communication data.

CONSTITUTION: A private key storage part 10 of communication equipment has a private key K uniquely decided for each piece of equipment. Address information uniquely decided for each piece of equipment, the address information of present equipment and open information or the like are previously possessed from an open list 20 and stored in an address storage part 12. A seal information generating part 13 transfers the **signature** found by calculation to a communication frame generating part 15 as seal information corresponding to communication information to be transmitted. According to an instruction from an operating part 11, the communication frame generating part 15 integrates seal information 26 corresponding to the communication information possessed from the seal information generating part 13 into a communication frame. A transmission part 16 sends the communication frame assembled by the communication frame generating part 15 to communication equipment Tj on the reception side while referring to a destination address part.

8/5/8 (Item 8 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

03899384 **Image available**
MULTIPLE DIGITAL **SIGNATURE** SYSTEM

PUB. NO.: 04-264484 [JP 4264484 A]

PUBLISHED: September 21, 1992 (19920921)
INVENTOR(s): OTA KAZUO
OKAMOTO TATSUAKI
FUJIOKA ATSUSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 03-024854 [JP 9124854]
FILED: February 19, 1991 (19910219)
INTL CLASS: [5] **G09C-001/00** ; G06F-015/00; H04L-009/00; H04L-009/10; H04L-009/12
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION -- Telegraphy); 45.4 (INFORMATION PROCESSING -- Computer Applications)
JOURNAL: Section: P, Section No. 1479, Vol. 17, No. 51, Pg. 71, February 02, 1993 (19930202)

ABSTRACT

PURPOSE: To provide the efficient multiple digital **signature** system which can reduce the memory capacity, throughput, and **communication** quantity **without** storing **signatures** individually by a verifier when many persons want to sign an electronic document in order.

CONSTITUTION: When plural signers 200...600 sign the electronic document in order, the signers 200...600 register keys in the open file at a center 100, keys for inspection are open to the public, and **signature** keys are controlled in secret. The signers 200...600 calculate **signature** components for a message by using the prime number of system common information and **signature** keys and sends them to the verifier 800 together with the message. The **signatures** are inspected by verifying whether the **signature** components are correct **signatures** or illegal **signatures** for the message by the verifiers 800 by using the keys for inspection given from the open file at the center 100.

8/5/9 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015769149 **Image available**
WPI Acc No: 2003-831351/200377
XRPX Acc No: N03-664326
Group signature **generation apparatus for secured business application, affixes electronic** signature **unique to group on message transmitted from member belonging to that group**
Patent Assignee: FUJI XEROX CO LTD (XERF)
Inventor: KUROSAKI M; TERAO N
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030188167	A1	20031002	US 2003340608	A	20030113	200377	B
JP 2003298576	A	20031017	JP 200298010	A	20020329	200377	

Priority Applications (No Type Date): JP 200298010 A 20020329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030188167	A1		13	H04L-009/00	
JP 2003298576	A		8	H04L-009/32	

Abstract (Basic): US 20030188167 A1

NOVELTY - A member authentication unit (102) authenticates each group member for identity, using an authentication message. An electronic **signature** generation unit (104) generates and affixes an electronic **signature** of the group to the message, when the authentication results is determined. A message transmitting unit (109) transmits the message with affixed electronic **signature** to a receiver.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) group **signature** generation method;
(2) group **signature** computer program; and
(3) mailing list server.
USE - Group **signature** generation apparatus for secured business application.
ADVANTAGE - Enables a job group member to **transmit** a message with a **signature** of the job group **without** holding a secret key of the job group, whereby the receiver can validate that the message is from the job group.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the group **signature** generation apparatus.
group **signature** service unit (10)
directory service unit (20)
archive service unit (30)
time stamp service unit (40)
member authentication unit (102)
signature generation unit (104)
message receiving unit (107)
message transmitting unit (109)
pp; 13 DwgNo 1/9
Title Terms: GROUP; **SIGNATURE** ; GENERATE; APPARATUS; SECURE; BUSINESS; APPLY; AFFIX; ELECTRONIC; **SIGNATURE** ; UNIQUE; GROUP; MESSAGE; TRANSMIT; MEMBER; BELONG; GROUP
Derwent Class: P85; T01
International Patent Class (Main): H04L-009/00; H04L-009/32
International Patent Class (Additional): G06F-015/00; **G09C-001/00** ; H04Q-007/38
File Segment: EPI; EngPI

8/5/10 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

[illegible]7285 **Image available**
[illegible] No: 2003-107801/200310
[illegible] No: N03-086323
Electronic signature **processing system divides calculation process of electronic** signature **, into** hash **and encryption processes, such that** hash **and encryption calculations are performed by server and terminal, respectively**
Patent Assignee: NEC CORP (NIDE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2002351316	A	20021206	JP 2001157312	A	20010525	200310	B

Priority Applications (No Type Date): JP 2001157312 A 20010525
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2002351316	A		9	G09C-001/00	

Abstract (Basic): JP 2002351316 A
NOVELTY - The calculation units (22,32) divide the calculation process performed with respect to electronic **signature** , into **hash** calculation process and encryption calculation process using secret key, such that the **hash** calculation and encryption calculation are performed respectively by a server (2) and a terminal (3).
USE - Electronic **signature** processing system.
ADVANTAGE - By processing the electronic **signature separately** in server and terminal side calculation units, **communication** cost and time are reduced. Enables the user to utilize managed secret key information.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the electronic **signature** processing system. (Drawing includes non-English language text).
Server (2)
Terminal (3)

Calculation unit (22,32)
pp; 9 DwgNo 1/8
Title Terms: ELECTRONIC; **SIGNATURE** ; PROCESS; SYSTEM; DIVIDE; CALCULATE; PROCESS; ELECTRONIC; **SIGNATURE** ; **HASH** ; ENCRYPTION; PROCESS; **HASH** ; ENCRYPTION; CALCULATE; PERFORMANCE; SERVE; TERMINAL; RESPECTIVE
Derwent Class: P85; T01; T05
International Patent Class (Main): **G09C-001/00**
International Patent Class (Additional): G06F-017/60
File Segment: EPI; EngPI

8/5/11 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013986024 **Image available**
WPI Acc No: 2001-470238/200151
XRPX Acc No: N01-349225
Mail server outputs electronic mail to destination after providing digital signature **to the mail**
Patent Assignee: NTT IDO TSUSHINMO KK (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001168902	A	20010622	JP 99350404	A	19991209	200151	B

Priority Applications (No Type Date): JP 99350404 A 19991209
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001168902	A		10	H04L-012/54	

Abstract (Basic): JP 2001168902 A
NOVELTY - A mail receiving unit receives electronic mail from mail client. A **signature** unit outputs digital **signature** to the electronic mail. Mail transmitting unit transmits electronic mail with digital **signature** to transmission destination.
USE - Mail server to which portable telephone is connected through mobile communication network.
ADVANTAGE - **Transmits** mail with digital **signature** to destination **without** increasing traffic of **transmission** path.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of electronic mail system used for mail server. (Drawing includes non-English language text).
pp; 10 DwgNo 1/7
Title Terms: MAIL; SERVE; OUTPUT; ELECTRONIC; MAIL; DESTINATION; AFTER; DIGITAL; **SIGNATURE** ; MAIL
Derwent Class: P85; T01; W01
International Patent Class (Main): H04L-012/54
International Patent Class (Additional): G06F-013/00; **G09C-001/00** ; H04L-009/32; H04L-012/58
File Segment: EPI; EngPI

8/5/12 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013746376 **Image available**
WPI Acc No: 2001-230605/200124
XRPX Acc No: N01-164339
Secret distributed **system generates decoding and** signature **results by combining information from arbitrary terminals among** distributed **terminals** without **computing secret key**
Patent Assignee: TOSHIBA KK (TOKE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001034164	A	20010209	JP 99209891	A	19990723	200124	B

Priority Applications (No Type Date): JP 99209891 A 19990723
Patent Details:
Patent No Kind Lan Pg   Main IPC   Filing Notes
JP 2001034164 A   19 G09C-001/00

Abstract (Basic): JP 2001034164 A
NOVELTY - The user terminal (U) is connected to distributed terminals (P1-Pn) through a network (1). Final information about secret key is partially distributed in each terminal. Decoding and **signature** results are generated by combining information from arbitrary terminals among n' terminals without computing secret key.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for memory medium.
USE - Secret distributed system.
ADVANTAGE - Decoding result is generated without need for secret key and portioner.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of secret distributed system.
Network (1)
Terminals (P1-Pn)
User terminal (U)
pp; 19 DwgNo 1/13
Title Terms: SECRET; DISTRIBUTE; SYSTEM; GENERATE; DECODE; **SIGNATURE** ; RESULT; COMBINATION; INFORMATION; ARBITRARY; TERMINAL; DISTRIBUTE; TERMINAL; COMPUTATION; SECRET; KEY
Derwent Class: P85; T01; W01
International Patent Class (Main): **G09C-001/00**
International Patent Class (Additional): G06F-012/14; H04L-009/08; H04L-009/10
File Segment: EPI; EngPI

8/5/13 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013560461 **Image available**
WPI Acc No: 2001-044668/200106
XRPX Acc No: N01-033773
Distribution management apparatus calculates signature **value corresponding to** hash **value of object flow information by using computed first and second** signature **values**
Patent Assignee: FUJI XEROX CO LTD (XERF)
Inventor: SHIN G H
Number of Countries: 002 Number of Patents: 003
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
JP 2000305995 A 20001102 JP 99115551 A 19990422 200106 B
KR 2000067788 A 20001125 KR 9945071 A 19991018 200130
KR 365348 B 20021218 KR 9945071 A 19991018 200336

Priority Applications (No Type Date): JP 99115551 A 19990422
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
JP 2000305995 A 42 G06F-017/60
KR 2000067788 A G06F-017/60
KR 365348 B G06F-017/60 Previous Publ. patent KR 2000067788

Abstract (Basic): JP 2000305995 A
NOVELTY - The **signature** value corresponding to the **hash** value of the object flow information is calculated by using the first and second **signature** values. A **signature** unit computes the first **signature** value to the **hash** value of the object flow information by using a signer confidential information.
DETAILED DESCRIPTION - An object flow information generator computes the second **signature** value to the **hash** value of the object flow information by using a **signature** key information. The signer

confidential information is taken out from a signer confidential information memory. A **signature** key information selector takes out the **signature** key information that corresponds to the product identifier from the **signature** key information memory. An INDEPENDENT CLAIM is also included for an information distribution management method.

USE - Used for performing the distribution management of goods.

ADVANTAGE - Enables **distribution** manufacturers to verify a **signature** **without** the necessity of acquiring the certificate for every signer from an authentication station. Prevents mischief since forgery of the identifications are prevented.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of the verification operation.

pp; 42 DwgNo 3/24

Title Terms: DISTRIBUTE; MANAGEMENT; APPARATUS; CALCULATE; **SIGNATURE** ; VALUE; CORRESPOND; **HASH** ; VALUE; OBJECT; FLOW; INFORMATION; COMPUTATION; FIRST; SECOND; **SIGNATURE** ; VALUE

Derwent Class: P85; Q35; T01

International Patent Class (Main): G06F-017/60

International Patent Class (Additional): B65G-001/137; G06K-017/00; **G09C-001/00** ; G09F-003/00

File Segment: EPI; EngPI

8/5/14 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012771386 **Image available**

WPI Acc No: 1999-577609/199949

XPIX Acc No: N99-426766

Data communication system - has communication apparatus (10) provided with authentication processor for determining correctness of data communication between communication apparatus and another communication apparatus

Patent Assignee: NTT DATA TSUSHIN KK (NITE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11252068	A	19990917	JP 9850722	A	19980303	199949	B

Priority Applications (No Type Date): JP 9850722 A 19980303

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11252068	A		10	H04L-009/32	

Abstract (Basic): JP 11252068 A

NOVELTY - A communication apparatus (10) in the data communication system (1) is provided with an authentication processor (14) for determining the correctness of the data communication between the communication apparatus and another communication apparatus. DETAILED DESCRIPTION - The authentication unit compares the electronic **signature** , decoded with a decoding key of the other communication apparatus specified by the address data, with the data for authentication. Either communication apparatus reads an IC card (20) which stores the data for authentication corresponding to an electronic **signature** generated by the address data on the other communication apparatus. The other **communication** apparatus has an intrinsic encryption key for the electronic **signature** . **INDEPENDENT** CLAIMS are also included for the following:the components of the data communication system;and the recording medium.

USE - None given.

ADVANTAGE - Enhances data communication efficiency in which data communication is established based on authentication data stored in a recording medium. Ensures safe and optimum access opposing specific communication apparatus from a remote area. DESCRIPTION OF DRAWING(S) - The figure shows the functional block diagram of the data communication system. (1) Data communication system; (10) Communication apparatus;

(14) Authentication processor; (20) IC card.
Dwg.1/7
Title Terms: DATA; COMMUNICATE; SYSTEM; COMMUNICATE; APPARATUS; AUTHENTICITY; PROCESSOR; DETERMINE; CORRECT; DATA; COMMUNICATE; COMMUNICATE; APPARATUS; COMMUNICATE; APPARATUS
Derwent Class: P76; P85; T01; W01
International Patent Class (Main): H04L-009/32
International Patent Class (Additional): B42D-015/10; G06F-013/368; **G09C-001/00**
File Segment: EPI; EngPI

8/5/15 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012677121 **Image available**
WPI Acc No: 1999-483228/199941
XRPX Acc No: N99-360258
Digital signature **system used by communication apparatus - confirms correctness of generated** signature **using disclosing data of authorized user within group, and distinguishes user which generated** signature **from random number used in generating** signature
Patent Assignee: CANON KK (CANO)
Inventor: OISHI K
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11202767	A	19990730	JP 986630	A	19980116	199941	B
US 6298153	B1	20011002	US 99229440	A	19990113	200160	

Priority Applications (No Type Date): JP 986630 A 19980116; JP 986629 A 19980116
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11202767	A		11	G09C-001/00	
US 6298153	B1			G06K-009/18	

Abstract (Basic): JP 11202767 A
NOVELTY - The correctness of the generated **signature** is confirmed using the disclosing data of the authorized user within the group. The user which generated the **signature** is then distinguished from the random number used in generating the **signature** . DETAILED DESCRIPTION - An intrinsic disclosing data is generated from a disclosure parameter common to each user and the confidential data of each user. New disclosing and confidential data are then generated as member data based on the public-presentation data intrinsic to an authorized member of a particular group. The generated member data are then secretly transmitted to a user within the group. The relationship of each generated member data are then confirmed as to whether or not predetermined conditions were met. Using the confirmed member data, a corresponding **signature** is generated.An **INDEPENDENT** CLAIM is also included for a data **communication** system.
USE - For communication apparatus.
ADVANTAGE - Improves safety by maintaining anonimity of generated **signature** even in situations by which comparison problems resulting from use of discrete logarithms occurs. Addition of new members is unnecessary when exchanging members within group. DESCRIPTION OF DRAWING(S) - The figure shows the component block diagram of the communication system.
Dwg.1/4
Title Terms: DIGITAL; **SIGNATURE** ; SYSTEM; COMMUNICATE; APPARATUS; CONFIRM; CORRECT; GENERATE; **SIGNATURE** ; DISCLOSE; DATA; USER; GROUP; DISTINGUISH; USER; GENERATE; **SIGNATURE** ; RANDOM; NUMBER; GENERATE; **SIGNATURE**
Derwent Class: P85; W01
International Patent Class (Main): G06K-009/18; **G09C-001/00**
International Patent Class (Additional): H04L-009/32
File Segment: EPI; EngPI

8/5/16 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012648638 **Image available**
WPI Acc No: 1999-454743/199938
XRPX Acc No: N99-340775
Interactive authentication for e.g. communication system - involves transmitting digital signature **of certificate in disclosure key corresponding to digital** signature **key of apparatus, towards another apparatus, to verify received certificate and** signature
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11191761	A	19990713	JP 97357158	A	19971225	199938	B
JP 3253060	B2	20020204	JP 97357158	A	19971225	200211	

Priority Applications (No Type Date): JP 97357158 A 19971225
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11191761	A		11	H04L-009/32	
JP 3253060	B2		12	H04L-009/32	Previous Publ. patent JP 11191761

Abstract (Basic): JP 11191761 A
NOVELTY - In order to verify the certificate and the digital **signature** received by communication apparatuses (STA1,STA2), the communication apparatus (STA2) transmits the digital **signature** of a certificate in a disclosure key corresponding to a digital **signature** key, towards the communication apparatus (STA1). DETAILED DESCRIPTION - The method involves authenticating the digital **signature** of a key disclosure authentication station corresponding to the digital **signature** key of a **communication** apparatus (STA1). Another digital **signature** key is **transmitted** to another **communication** apparatus (STA2). An **INDEPENDENT** CLAIM is also included for an interactive authenticating apparatus.
USE - For e.g. communication system.
ADVANTAGE - Prevents incorrect authentication of certificate disclosure key corresponding to secret key. Ensures efficient interactive authentication procedure. DESCRIPTION OF DRAWING(S) - The figure shows the sequence diagram of an interactive authentication procedure. (STA1,STA2) Communication apparatuses.
Dwg.1/8
Title Terms: INTERACT; AUTHENTICITY; COMMUNICATE; SYSTEM; TRANSMIT; DIGITAL ; **SIGNATURE** ; CERTIFY; DISCLOSE; KEY; CORRESPOND; DIGITAL; **SIGNATURE** ; KEY; APPARATUS; APPARATUS; VERIFICATION; RECEIVE; CERTIFY; **SIGNATURE**
Derwent Class: P85; W01
International Patent Class (Main): H04L-009/32
International Patent Class (Additional): **G09C-001/00** ; H04L-009/08
File Segment: EPI; EngPI

8/5/17 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012344 **Image available**
WPI Acc No: 1998-449254/199839
XRPX Acc No: N98-350362
Identification method for controlling access to server services - involves identifying client from database or signature **and referencing access rules from database to manage request**
Patent Assignee: XCERT SOFTWARE INC (XCER-N)
Inventor: CSINGER A; KNIPE B; RICHARD P; WOODWARD B
Number of Countries: 028 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 862105	A2	19980902	EP 98301300	A	19980223	199839	B
AU 9856278	A	19980903	AU 9856278	A	19980225	199847	
CA 2230304	A	19980828	CA 2230304	A	19980223	199903	
JP 10308733	A	19981117	JP 9847343	A	19980227	199905	
US 5922074	A	19990713	US 97808846	A	19970228	199934	
US 6249873	B1	20010619	US 97808846	A	19970228	200137	
			US 99352353	A	19990713		
AU 739898	B	20011025	AU 9856278	A	19980225	200173	

Priority Applications (No Type Date): US 97808846 A 19970228; US 99352353 A 19990713

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 862105	A2	E	19	G06F-001/00	
Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
AU 9856278	A			H04L-009/30	
CA 2230304	A			H04L-009/30	
JP 10308733	A		19	H04L-009/32	
US 5922074	A			G06F-011/00	
US 6249873	B1			G06F-012/14	Div ex application US 97808846 Div ex patent US 5922074
AU 739898	B			H04L-009/30	Previous Publ. patent AU 9856278

Abstract (Basic): EP 862105 A

The distributed system has a number of clients that make requests upon servers. Access to the server has constraints related to the identity of the client. A client (40) communicates with a server (42) over an underlying secure communications protocol (2a). The server checks (2b) in an internal database (50) if the client is known, and if so the database returns (2c) access control rules for the client. These rules then condition the client communications (2d).

The client identity is known from the secure protocol and may include the use of **signatures** . If the **signature** is not in the database, its originator can be referenced.

ADVANTAGE - Provides secure **communication** and **signature** verification **without** requiring a global certification authority.

Dwg.2/13

Title Terms: IDENTIFY; METHOD; CONTROL; ACCESS; SERVE; SERVICE; IDENTIFY; CLIENT; DATABASE; **SIGNATURE** ; REFERENCE; ACCESS; RULE; DATABASE; MANAGE; REQUEST

Derwent Class: P85; T01; W01

International Patent Class (Main): G06F-001/00; G06F-011/00; G06F-012/14; H04L-009/30; H04L-009/32

International Patent Class (Additional): G06F-013/00; **G09C-001/00** ; H04L-012/12; H04L-012/16; H04L-029/06

File Segment: EPI; EngPI

8/5/18 **(Item 10 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011473207 **Image available**

WPI Acc No: 1997-451114/199742

XRPX Acc No: N97-375846

Demonstration of time of execution of cryptographic transaction - using comparison of times recorded by radio controlled clock, and preferably crystal clock, in common module with antenna and battery

Patent Assignee: DEUT TELEKOM AG (DEBP)

Inventor: HUBER K; TOENSING F

Number of Countries: 022 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 795979	A2	19970917	EP 97101090	A	19970124	199742	B
DE 19610401	A1	19970918	DE 1010401	A	19960316	199743	
JP 10020782	A	19980123	JP 9759708	A	19970314	199814	

CA 2200037	A	19970916	CA 2200037	A	19970314	199815
US 5781630	A	19980714	US 97818464	A	19970317	199835
IL 120436	A	20000229	IL 120436	A	19970313	200029

Priority Applications (No Type Date): DE 1010401 A 19960316
Cited Patents: No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 795979	A2	G	5	H04L-009/32	
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
DE 19610401	A1		5	H04L-009/32	
JP 10020782	A		5	G09C-001/00	
IL 120436	A			H04K-001/00	
CA 2200037	A			G06F-017/60	
US 5781630	A			H04L-009/00	

Abstract (Basic): EP 795979 A

The method involves using a computer (2) interfaced (3) to a module (1) in which a processor (4) with memory (5) is linked to a radio clock (6) and a battery-powered crystal clock (8). A document prepared in the computer is encrypted and signed by the processor before being transmitted.

The time markings are supplied by both clocks and compared. If the discrepancy is less than a predetermined maximum, the time entered by the radio clock is applied to the document, encrypted, and if necessary signed together with it.

ADVANTAGE - Time of **signature** , presentation, **transmission** or reception of any document can be established reliably, **without** possibility of falsification by originator.

Dwg.1/1

Title Terms: DEMONSTRATE; TIME; EXECUTE; CRYPTOGRAPHIC; TRANSACTION; COMPARE; TIME; RECORD; RADIO; CONTROL; CLOCK; PREFER; CRYSTAL; CLOCK; COMMON; MODULE; ANTENNA; BATTERY
Derwent Class: P85; S04; T01; W01
International Patent Class (Main): G06F-017/60; **G09C-001/00** ; H04K-001/00; H04L-009/00; H04L-009/32
International Patent Class (Additional): G04C-011/02; G06F-015/00; G06K-019/073; H04L-009/10
File Segment: EPI; EngPI

8/5/19 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

011468514 **Image available**
WPI Acc No: 1997-446421/199741
XRPX Acc No: N97-372042

Signature **correctness confirmation appts used during utilisation of certain services such as viewing computer program - receives encrypted information and utilisation information which are coupled and used with individual key to perform** signature **calculation**

Patent Assignee: FUJI XEROX CO LTD (XERF)
Inventor: ARATANI T; KOBAYASHI K; SHIN K
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9205424	A	19970805	JP 9611568	A	19960126	199741	B
JP 2991099	B2	19991220	JP 9611568	A	19960126	200005	
US 6072874	A	20000606	US 96777047	A	19961230	200033	

Priority Applications (No Type Date): JP 9611568 A 19960126
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9205424	A		13	H04L-009/32	
JP 2991099	B2		14	G09C-001/00	Previous Publ. patent JP 9205424
US 6072874	A			H04N-007/167	

Abstract (Basic): JP 9205424 A

The appts is used to confirm a **signature** when an user signs the information relating to the utilisation of a source which is offered in a format that is utilised only with a key information. The utilisation information for a **signature** , is formed by a **signature** information issue unit (22). A coupling calculation unit (34) receives the encrypted key information and the utilisation information and performs a first calculation. A **signature** calculation unit (30) receives the result of the first calculation and uses the user's individual key to perform a **signature** calculation.

The execution result is returned to an isolation calculation unit of the information issue unit. The isolation calculation unit uses the key information and the signal link information and isolates the information to a signed utilisation information.

USE/ADVANTAGE - For confirming **signature** of person utilising **broadcast** services. Improves calculation efficiency. Enables confirming correctness of **signature** **without** verifying digital **signature** .

Dwg.1/4

Title Terms: **SIGNATURE** ; CORRECT; CONFIRM; APPARATUS; UTILISE; SERVICE; VIEW; COMPUTER; PROGRAM; RECEIVE; ENCRYPTION; INFORMATION; UTILISE; INFORMATION; COUPLE; INDIVIDUAL; KEY; PERFORMANCE; **SIGNATURE** ; CALCULATE

Derwent Class: P85; T01; W01

International Patent Class (Main): **G09C-001/00** ; H04L-009/32; H04N-007/167

International Patent Class (Additional): G06F-009/06; G06F-012/14

File Segment: EPI; EngPI

01698439 SUPPLIER NUMBER: 16219952 (THIS IS THE FULL TEXT)

Firm has technology you can bank on; with "digital cash," transactions made over public networks remain secure and private. (Tech View) (DigiCash BV's electronic cash)

Sullivan, Eamonn

PC Week, v11, n34, p83(3)
August 29, 1994
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1758 LINE COUNT: 00135

ABSTRACT: DigiCash BV of Amsterdam is removing one of the biggest obstacles to keeping financial transactions over networks secure by licensing its electronic cash (e-cash) system to financial institutions. E-cash is a safe replacement to hard currency and also guards against controls large corporations potentially have over electronic transactions. Unlike credit and debit cards that offer little security, e-cash makes use of public key or digital signatures, which are safer and well-adapted for network uses including Internet. The user creates both a public and private key. The public key is widely proliferated, while the private key is guarded. Users actually make the money themselves and their financial institution must then validate it. The user could create e-cash notes in chosen denominations and assign each a random security number. One possible problem with the system is the same note could be used more than once.

TEXT:

One of the last barriers to the widespread use of public computer networks for commerce has been the difficulty of keeping financial transactions secure and private.

However, a Dutch-based company has developed a secure replacement for hard currency that also protects against the Orwellian-like control that electronic transactions could give to large banks and other financial institutions.

DigiCash BV of Amsterdam is licensing the basic technology for digital, electronic cash (called E-cash for short) to financial institutions and other large companies. DigiCash also hopes later this year to release free software (for PCs running Windows and for Macintoshes) based on its technology.

DigiCash is not the only outfit interested in helping put financial transactions on-line. Earlier this month, the U.S. Postal Service expressed an interest in playing a role in electronic commerce.

Those who would like to try DigiCash's software can ask to be included in beta testing, which began at the end of last month. The E-mail address for would-be beta testers is ecashbeta@digicash. support.nl.

David Chaum, DigiCash's managing director, outlined the E-cash technology at the World-Wide Web conference in Geneva in May. The company also has hardware-based payment schemes that use the same basic technology as digital cash, and has implemented these on a small scale, but its digital cash is the first software-only product to use the technology.

Privacy

Replacements for cash are, of course, nothing new. Credit cards and debit cards have been in use for years. However, they have relatively poor security (in the case of debit cards, just a four-number personal identification number) and their use is easily tracked.

The latter problem is of growing concern to consumers, as it becomes more apparent that an unacceptably large number of organizations can get very detailed personal information about an individual just by using the traceable records produced by credit and debit cards.

Electronic transactions are often much more efficient, however, so they are likely to become more common. To avoid further erosion of privacy, a system as anonymous as cash transactions -- with the efficiency of electronic transactions -- is needed.

Public key signatures

At its core, E-cash uses public key signatures, or digital signatures, which are both very secure and well-suited for use on public

networks (such as a telephone system or the Internet) because they can be used without requiring so-called "secure" or untappable channels.

Public key signatures are one manifestation of public key cryptography systems, which were first developed in the 1970s at Stanford University and the Massachusetts Institute of Technology. The secret part of the encryption scheme (the private key that deciphers encrypted messages or signatures) is never transmitted between the sender and receiver.

Instead, the sender (or signer, in the case of E-cash) generates both a private and a public key. The public key is disseminated as widely as possible, but the private key remains secret. Any message encrypted with one of the two keys can only be deciphered with the other.

To "sign" an electronic message, the signer generates a number based on the contents of the document (typically with some kind of hash function or checksum) and then encrypts that number with his or her private key. The **signature** can be embedded in a document or **sent** in a **separate** file.

To verify that a document was signed by the sender and has not been altered since it was signed, the recipient looks up the signer's public key (which will probably be available in an on-line database at some point), uses the same formula as the sender to generate a number from the document's contents, and then decrypts the signature using the sender's public key. If the number generated from the document and the number decrypted in the signature are equal, then the signature is valid.

In the E-cash system, the "currency" itself would bear the signature of the bank or other financial institution that issued the E-cash. That signature could be checked by a merchant for authenticity using the bank's public key. Digital signatures would also be used by the bank's customers for withdrawals and by merchants for deposits. (The public keys might, in fact, be stored by the Postal Service. The Postal Service is developing postal electronic services to issue public key certificates and store them in a public directory, officials said earlier this month.)

Withdrawing bank notes

With E-cash, consumers would essentially make the "money" themselves, then get their bank (or other financial institution) to authenticate it. This is similar to writing a personal check, except the merchant would not need to verify the identity of the person.

The consumer would generate E-cash notes in whatever denominations necessary and attach a random number to each of them. The random number would have to be of a sufficient size to make the chance of duplication negligible (100 digits would be sufficient), but in the E-cash system it is important that the consumer (or the consumer's computer) be the one to generate the numbers.

Consumers would then sign the E-cash notes with their digital signature and submit them to the bank. The bank would check the validity of the digital signature, deduct the amount of the E-cash notes from the consumer's account, and then sign the notes with the bank's digital signature before sending them back to the consumer.

When E-cash is used to purchase something, merchants would check the authenticity of the notes by checking the signatures against the bank's public keys. The notes would then be sent back to the bank by the merchant. The bank would check the authenticity of its own signature, would credit the merchant's account (after checking the merchant's attached signature), and, as an option, might send back a signed receipt.

Every step in this process can be done over a public network. Obtaining the public key of any of the participants by methods such as wiretapping would not weaken the system's security in any way, because the corresponding private keys are needed to decipher signatures or to create valid digital signatures.

Contrast this with the way credit cards are used. If someone intercepts a credit-card number and the name of its user, he or she can use that number to make purchases. Listening in on an E-cash transaction gains the eavesdropper nothing.

Anonymity

The system as described so far is secure, but the bank would still be able to track exactly where its customers were spending their money. This is where the random numbers become more important.

Before submitting the E-cash notes to the bank, the consumer would multiply the random numbers on the notes by a factor known only to the consumer. After the notes were signed by the bank, the consumer would

divide the numbers on the bank notes by the same factor previously used as a multiplier. Because of the mathematics of public-key cryptography, the bank's signature on the authenticated notes would still be irrefutably valid, but the bank would now have no record of which customer had which notes (much as banks have no record of which customer has which particular $5 or $20 bill).

Aside from giving the consumer anonymity, the random numbers used to mark the E-cash could also be used to trace the money in the case of theft. If a user's computer were stolen, the E-cash stored on it could be used by anyone.

After the theft, however, the user could supply the bank with the multiplier used on the random number. The bank could use that multiplier to calculate the real number on the stolen E-cash. Armed with that identifying number, the bank could then trace the E-cash if it were used by the thief.

The system thus has the advantages of cash and credit cards: An E-cash payment is as anonymous as cash unless its owner chooses to have it traced; then it becomes as easy to follow as a credit card transaction.

Another advantage is that consumers could use a different digital pseudonym (with its own verifiable signature) at each institution with which they do business -- making large-scale, cross-indexed consumer databases (used today by anyone with access to Social Security numbers) next to impossible.

Remaining problems

A couple of problems remain with this system. One is the possibility that the same note could be spent more than once. DigiCash has built a rather complex mathematical check into the system to make sure notes are traceable if they are used more than once.

More proactive solutions (intended to stop double spending before it happens) are even more complex and involve special "observer" chips or processes that could be validated by some authority, such as a government regulatory agency.

Such chips or processes would have to be built into the computer that does the E-cash transactions, so this solution is only suitable for hardware-based systems (such as handheld computers that are used as electronic wallets).

A more vexing problem is how to encourage large retailers and financial institutions to use the new private system when they get so much benefit (marketing information and so forth) from the current system.

DigiCash argues that financial institutions would save an enormous amount on record keeping (counting cash, tracking credit slips, and making numerous transactions with credit-card companies), and that they would save an equally large amount on efforts now made to combat fraud.

The same system of digital signatures might also be used in numerous other areas. Diplomas, drivers' licenses, letters of credit, and other documents that are used for authentication and to judge credit worthiness could be validated less intrusively and with greater certainty using public and private keys and signatures.

DigiCash can be reached in the Netherlands at 31-20-665-2611. Readers can get more information by sending mail to info digicash.nl or on the World-Wide Web at http://digicash.support.nl/.

12/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

07040622 **Image available**
CHARACTER INFORMATION TRANSMISSION SYSTEM

PUB. NO.: 2001-268256 [JP 2001268256 A]
PUBLISHED: September 28, 2001 (20010928)
INVENTOR(s): TOMINO TAKENORI
APPLICANT(s): KYOCERA CORP
APPL. NO.: 2000-076647 [JP 200076647]
FILED: March 17, 2000 (20000317)
INTL CLASS: H04M-011/00; **G06F-013/00** ; H04M-001/00; H04M-001/57

ABSTRACT

PROBLEM TO BE SOLVED: To provide a character information transmission system that interlocks setting of a caller number notice with setting for attaching/ **not - attaching** a **signature** .

SOLUTION: The character information **transmission** system **transmits** character information to which **signature** data are attached, when the caller number notice is set and the **signature** data to be attached are registered at the transmission of the character information.
COPYRIGHT: (C)2001,JPO

12/5/2 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015778305 **Image available**
WPI Acc No: 2003-840507/200378
Card payment method with only a secret number without **a customer's** signature **on a printed sale slip and to** transfer **the payment amount to an account of an affiliated store**
Patent Assignee: LEE M G (LEEM-I)
Inventor: LEE M G
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2003042933	A	20030602	KR 200173818	A	20011126	200378	B

Priority Applications (No Type Date): KR 200173818 A 20011126
Parent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2003042933	A		1	G06F-017/60	

Abstract (Basic): KR 2003042933 A

NOVELTY - A card payment method is provided to process a card payment with only a secret number **without** a customer's **signature** on a printed sale slip and to **transfer** the payment amount to an account of an affiliated store as soon as the card is normally approved.

DETAILED DESCRIPTION - An affiliated store selects a card payment menu at a payment processing terminal(700), and the payment processing terminal requests an access to a server of a service provider(710). The server of the service provider approves the access request from the payment processing terminal(720). The payment processing terminal reads the data on the card of a customer if it is inserted into a slot of the terminal(730), and receives a secret number of the card and the payment amount(740, 750). The terminal transmits the card data, the secret number and the payment amount to the server of the service provider(760), and then the server of the service provider transmits the received data and the data on the affiliated store to a server of a card company for requesting a transaction approval(780). The server of the card company checks the credit of the customer(790), transmits the check result to the server of the service provider(800). If the credit of the customer is normal, the server of the card company instantly

transfers the payment amount to the account of the affiliated store(850). The card processing terminal receives the credit check result(810) and displays it(820).

pp; 1 DwgNo 1/10

Title Terms: CARD; PAY; METHOD; SECRET; NUMBER; CUSTOMER; **SIGNATURE** ; PRINT; SALE; SLIP; TRANSFER; PAY; AMOUNT; ACCOUNT; STORAGE

Derwent Class: T01; T05

International Patent Class (Main): **G06F-017/60**

File Segment: EPI

12/5/3 **(Item 2 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015741029 **Image available**

WPI Acc No: 2003-803230/200375

XRPX Acc No: N03-643889

Information transfer concurrency increasing method in object-based data storage system, involves configuring executable applications to access hash component for respective information transfer operation, on per-access basis

Patent Assignee: PANASAS INC (PANA-N)

Inventor: ZELENKA J D

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030187866	A1	20031002	US 2002368796	P	20020329	200375	B
			US 2002372044	P	20020412		
			US 2002274243	A	20021018		

Priority Applications (No Type Date): US 2002274243 A 20021018; US 2002368796 P 20020329; US 2002372044 P 20020412

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030187866	A1		13	G06F-017/00	Provisional application US 2002368796
					Provisional application US 2002372044

Abstract (Basic): US 20030187866 A1

NOVELTY - A directory object containing multiple entries is divided into **hash** components storing a respective non- overlapping portion of the entries. A **hash** master containing different entries pointing to different **hash** components is created. Executable applications are configured to access the **hash** component which is determined using a mapping function for respective information transfer operation on per-access basis.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) computer-readable storage medium storing program code for providing increased concurrency among information transfer operation; and

(2) object-based data storage system.

USE - In object-based data storage system (claimed), for providing increased concurrency among information transfer operation performed by executable application.

ADVANTAGE - The problem of access serialization is alleviated, while reducing data access latency and contention. The creation of **hash** components and **hash** master allows more than one client application or file manager, to concurrently access corresponding **hash** components for information **transfer** operation on stored objects, **without** creating access contentions.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the method of providing increased concurrency among information transfer operations performed by executable operations operating in an object-based data storage system.

pp; 13 DwgNo 5/6

Title Terms: INFORMATION; TRANSFER; INCREASE; METHOD; OBJECT; BASED; DATA;

STORAGE; SYSTEM; EXECUTE APPLY; ACCESS; **HASH** ; COMPONEI RESPECTIVE; INFORMATION; TRANSFER; OPERATE; PER; ACCESS; BASIS
Derwent Class: T01
International Patent Class (Main): **G06F-017/00**
File Segment: EPI

12/5/4 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014929221 **Image available**
WPI Acc No: 2002-749930/200281
XRPX Acc No: N02-590607
Lookup engine for network device, selects identity independent distribution hash **index from shift control logic, so that address table is used to output packet forward information for incoming packet**
Patent Assignee: CHEN J (CHEN-I); WANG Y (WANG-I)
Inventor: CHEN J; WANG Y
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020116527	A1	20020822	US 2000740819	A	20001221	200281	B

Priority Applications (No Type Date): US 2000740819 A 20001221
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020116527	A1		9	G06F-015/16	

Abstract (Basic): US 20020116527 A1
NOVELTY - A parser (11) acquires an address information of an incoming packet, corresponding to which a predetermined number of shift control logic (14,18) are produced. A selector selects an identity **independent distribution** (I.I.D) **hash** index from shift control logic, so that an address table is used to output forwarding information for the incoming packet.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for look up information generating method.
USE - Lookup engine for network device.
ADVANTAGE - Enables supporting packet forwarding mechanism reliably. Reduces the chance of the collision and improves the efficiency. A simple hardware implementation is provided for looking up an address table. Enables using the memory more efficiently within a short time.
DESCRIPTION OF DRAWING(S) - The figure shows a functional block diagram of the lookup engine.
Parser (11)
Shift control logic (14,18)
pp; 9 DwgNo 2/4
Title Terms: ENGINE; NETWORK; DEVICE; SELECT; IDENTIFY; INDEPENDENT; DISTRIBUTE; **HASH** ; INDEX; SHIFT; CONTROL; LOGIC; SO; ADDRESS; TABLE; OUTPUT; PACKET; FORWARD; INFORMATION; INCOMING; PACKET
Derwent Class: T01; U21; W01
International Patent Class (Main): **G06F-015/16**
File Segment: EPI

12/5/5 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014750713 **Image available**
WPI Acc No: 2002-571417/200261
XRPX Acc No: N02-452678
Authentication system has pair of transmitters **for** transmitting **request of** signature **input and authentication result to server** separately
Patent Assignee: CANON KK (CANO)

Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2002197067	A	20020712	JP 2000395850	A	20001226	200261	B

Priority Applications (No Type Date): JP 2000395850 A 20001226
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2002197067	A		6	G06F-015/00	

Abstract (Basic): JP 2002197067 A

NOVELTY - A server (100) has a database (101) storing the **signatures** of a user on an access request by a client, a transmitting unit (203) transmits a response requesting **signature** input of the user. On reception of the **signature** input, another transmitter (206) transmits result of authentication to the server and user.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Authentication control method;

(2) Computer readable memory storing authentication program; and

(3) Authentication program.

USE - Authentication system for performing authentication for clients for access to server.

ADVANTAGE - A sign authentication is performed safely.

DESCRIPTION OF DRAWING(S) - The figure shows the functional structure of the sign authentication system. (Drawing includes non-English language text).

Server (100)

Database (101)

Transmitters (203,206)

pp; 6 DwgNo 2/3

Title Terms: AUTHENTICITY; SYSTEM; PAIR; TRANSMIT; TRANSMIT; REQUEST; **SIGNATURE** ; INPUT; AUTHENTICITY; RESULT; SERVE; SEPARATE
Derwent Class: T01
International Patent Class (Main): **G06F-015/00**
File Segment: EPI

12/5/6 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013967011 **Image available**
WPI Acc No: 2001-451225/200148
XRPX Acc No: N01-334122

Failed software object authentication analysis by estimating if corruption is due to object or separate signatures **, by comparing** signature **value from inverse transformation function with message** signature **value**

Patent Assignee: GEN INSTR CORP (GENN)
Inventor: SAFADI R
Number of Countries: 095 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200116673	A1	20010308	WO 2000US23651	A	20000829	200148	B
AU 200069443	A	20010326	AU 200069443	A	20000829	200148	
EP 1210677	A1	20020710	EP 2000957888	A	20000829	200253	
			WO 2000US23651	A	20000829		
CN 1384930	A	20021211	CN 2000814952	A	20000829	200324	
TW 497021	A	20020801	TW 2000117439	A	20000829	200330	

Priority Applications (No Type Date): US 99389107 A 19990902
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200116673	A1	E	45	G06F-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT

RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW
AU 200069443 A G06F-001/00 Based on patent WO 200116673
EP 1221077 A1 E G06F-001/00 Based on patent WO 200116673
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SI
CN 1384930 A G06F-001/00
TW 497021 A G06F-001/00

Abstract (Basic): WO 200116673 A1

NOVELTY - A software object **signature** value (S) is extracted from a message m(s) with value (s). An object **signature** value (s') and value v' of secrete **signature** transformation function f(s) are extracted from object. A **signature** value (s'') is generated by applying inverse function f(s)-1 to v and is compared with s and s'. Message **signature** value or object is set as suspect, if s''=s' and if s''=s, respectively.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for user terminal for receiving and authenticating software objects from communication network.

USE - For detecting suspect object **signatures** and suspect software objects including application code, operating systems and associated components, basic input-output structures (BIOS), Java virtual machines (JVM), Java applications and Applets, etc., residing in digital set top terminals for cable and satellite television.

ADVANTAGE - Determines whether a failed authentication is resulted from corruption in the **downloaded** object or from corruption of the **separately communicated signature** for the **downloaded** object. A value indicative of the software object transmission facility is generated by the compact transformation function that operates on **signature** . Actual or attempted attacks on the security of the scheme used to download the software object is analyzed.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of the authentication failure detection method.

pp; 45 DwgNo 5/6

Title Terms: FAIL; SOFTWARE; OBJECT; AUTHENTICITY; ANALYSE; ESTIMATE; CORRUPT; OBJECT; SEPARATE; **SIGNATURE** ; COMPARE; **SIGNATURE** ; VALUE; INVERSE; TRANSFORM; FUNCTION; MESSAGE; **SIGNATURE** ; VALUE
Derwent Class: T01
International Patent Class (Main): **G06F-001/00**
File Segment: EPI

12/5/7 **(Item 6 from file: 350)**
File 350:Derwent WPIX
Thomson Derwent. All rts. reserv.

Image available
Acc No: 2001-006531/200101
Related WPI Acc No: 1999-180566; 2001-407770; 2002-179042
XRPX Acc No: N01-004682

Session management method over stateless protocol of internet communications, involves associating two requests, when total statistical significance calculated for identifiers exceeds preset significance level

Patent Assignee: TRIVNET LTD (TRIV-N); WILF S (WILF-I)
Inventor: WILF S
Number of Countries: 090 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200049528	A1	20000824	WO 2000IL94	A	20000216	200101	B
AU 200025700	A	20000904	AU 200025700	A	20000216	200103	
US 6496824	B1	20021217	US 99253137	A	19990219	200307	

Priority Applications (No Type Date): US 99253137 A 19990219
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200049528	A1	E	18	G06F-017/30	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

AU	200025700	A	G06F-017/30	Based on patent WO 200049528
US	6496824	B1	G06F-017/30	

Abstract (Basic): WO 200049528 A1

NOVELTY - First and second requests containing several first and second identifiers are received respectively. The several first identifiers are compared with several second identifiers. The first request and second request are associated when a total statistical significance calculated for the identifiers, is detected to be greater than a preset required significance level and when the comparison is successful.

DETAILED DESCRIPTION - A **hash** is generated for one of the several identifiers. If the generated **hash** is incompatible with previously generated **hashes** , information is associated with the generated **hash** based on which a response is sent, else, a response is **sent** based upon information previously associated with the previously generated **hash** . An **INDEPENDENT** CLAIM is also included for token for session management.

USE - For session management of internet communications over stateless protocol.

ADVANTAGE - Allows for faster and easier development by hashing the concatenated string. Enables estimating the popularity of each browser type or the server can calculate this over time by recording each HTTP request into an historical statistical database. Fingerprint provides stronger identification which is obtained by digitally hashing the identifiers, by enabling larger collection of identifiers. Allows the application designer to limit its error rate is quantifiable way.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of method for HTTP session management.

pp; 18 DwgNo 2/3

Title Terms: SESSION; MANAGEMENT; METHOD; PROTOCOL; COMMUNICATE; ASSOCIATE; TWO; REQUEST; TOTAL; STATISTICAL; SIGNIFICANT; CALCULATE; IDENTIFY; PRESET; SIGNIFICANT; LEVEL

Derwent Class: T01

International Patent Class (Main): **G06F-017/30**

File Segment: EPI

12/5/8 **(Item 7 from file: 350)**

013465053 **Image available**

WPI Acc No: 2000-636996/200061

XRPX Acc No: N00-472294

Software licensing method for electronic distribution in computer system, involves generating digital signature **for license using public or private keys and transmitting to user**

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)

Inventor: KNUTSON J I

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6078909	A	20000620	US 97974379	A	19971119	200061	B

Priority Applications (No Type Date): US 97974379 A 19971119

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6078909	A		11	G06F-017/60	

Abstract (Basic): US 6078909 A

NOVELTY - Public and private keys compatible for use with digital

signature algorithm A) for license for selected electronic distribution, are generated at licenser. A digital **signature** for license using one of the keys, is generated at licenser and transmitted to user. The license is verified by user using DSA for digital **signature** , license data and different one of keys **without** any **transmission** with licenser.

DETAILED DESCRIPTION - Only the public key is distributed to the user in electronic distribution and the private key is retained for generation of digital **signature** for license. Digital **signature** is generated by providing information to DSA including data for license terms for license. The license is verified by generating a true/false indication by DSA for license using the public key. INDEPENDENT CLAIMS are also included for the following:

(a) software licensing apparatus for electronic distribution in computer system;

(b) computer program product

USE - For licensing software for electronic distribution such as documents, letters, graphic images of computer system.

ADVANTAGE - Offers simple, low-cost software licensing method by utilizing digital **signature** software.

DESCRIPTION OF DRAWING(S) - The figure shows the computer network utilizing the software licensing method.

pp; 11 DwgNo 8/8

Title Terms: SOFTWARE; METHOD; ELECTRONIC; DISTRIBUTE; COMPUTER; SYSTEM; LICENSE; DIGITAL; **SIGNATURE** ; LICENCE; PUBLIC; PRIVATE; KEY; TRANSMIT; USER

Derwent Class: T01

International Patent Class (Main): **G06F-017/60**

File Segment: EPI

12/5/9 **(Item 8 from file: 350)**

013120324 **Image available**

WPI Acc No: 2000-292195/200025

XRPX Acc No: N00-219111

Method for preparing safe electronic document in electronic commerce, involves comparing decoded document with one without digital signature **to obtain message**

Patent Assignee: KOREA ELECTRONICS & TELECOM RES INST (KOEL-N); KOREA ELECTRONICS & TELECOM RES (KOEL-N); ELECTRONICS & TELECOM RES INST (ELTE-N)

Inventor: KIM T K; PARK C S; TARK S W; KIM T G; TAK S W

Number of Countries: 002 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6039248	A	20000321	US 986904	A	19980114	200025	B
KR 99033789	A	19990515	KR 9755208	A	19971027	200031	
KR 241350	B1	20000201	KR 9755208	A	19971027	200118	

Priority Applications (No Type Date): KR 9755208 A 19971027

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6039248	A		13	G06F-017/60	
KR 99033789	A			G06F-019/00	
KR 241350	B1			G06F-019/00	

Abstract (Basic): US 6039248 A

NOVELTY - An electronic notarized document is transmitted with digital **signature** to customer (10) or merchant (20). The document is then decoded and transmitted with digital **signature** to notarization organization (60). The decoded document is then compared with document **without** digital **signature** to obtain message of document. The document is then **sent** with digital **signature** to customer or merchant and then stored.

DETAILED DESCRIPTION - A primary electronic notarized document is

prepared based on transaction detail information, a customer certificate, merchant certificate, notarizing organization certificate and certifying organization certificate. A digital **signature** is put in the notarized document by using private key so as to form a secondary electronic notarized document which is then transmitted to a customer merchant. The secondary electronic notarized document is decoded and a digital **signature** is put on it using private key so as to form tertiary document. The tertiary document is then transmitted to notarizing organization and is decoded using an open key to form a biquadratic electronic document. This document is then compared with primary document and a message of notarized document finding correspondence between primary and biquadratic documents is obtained. A digital **signature** is then put on the message using a private key. A final document is formed for providing realization of transaction by utilizing digitally signed tertiary document.

USE - In E-commerce.

ADVANTAGE - Authenticity of transaction document is ensured due to use of digital **signature** . Safety in transaction is increased as denial of reception or transmission of transaction are prevented.

DESCRIPTION OF DRAWING(S) - The figure shows the electronic transaction using certificate techniques.

Customer (10)

Merchant (20)

Notarization organization (60)

pp; 13 DwgNo 2/8

Title Terms: METHOD; PREPARATION; SAFE; ELECTRONIC; DOCUMENT; ELECTRONIC; COMPARE; DECODE; DOCUMENT; ONE; DIGITAL; **SIGNATURE** ; OBTAIN; MESSAGE

Derwent Class: T01; T05; W01

International Patent Class (Main): **G06F-017/60** ; **G06F-019/00**

International Patent Class (Additional): H04K-001/00

File Segment: EPI

12/5/10 **(Item 9 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

012374451 **Image available**

WPI Acc No: 1999-180558/199915

XRPX Acc No: N99-132608

Detection method for computer viruses spanning multiple data streams - processor scans data streams for components of virus, and scan results are used by processor to evaluate Boolean expression in order to determine existence of virus

Patent Assignee: SYMANTEC CORP (SYMA-N)

Inventor: CHI D

Number of Countries: 022 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9908189	A1	19990218	WO 98US13774	A	19980630	199915	B
US 6006329	A	19991221	US 97909203	A	19970811	200006	
EP 1012719	A1	20000628	EP 98934236	A	19980630	200035	
			WO 98US13774	A	19980630		
EP 1012719	B1	20020904	EP 98934236	A	19980630	200266	
			WO 98US13774	A	19980630		
DE 69807716	E	20021010	DE 607716	A	19980630	200274	
			EP 98934236	A	19980630		
			WO 98US13774	A	19980630		

Priority Applications (No Type Date): US 97909203 A 19970811

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9908189	A1	E	32	G06F-011/00	

Designated States (National): CA JP

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

US 6006329	A		G06F-012/14	
EP 1012719	A1	E	G06F-011/00	Based on patent WO 9908189

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
EP 1012719 B1 E G06F-011/00 Based on patent WO 9908189
Designated States (Regional): DE FR GB
DE 69807716 E G06F-011/00 Based on patent EP 1012719
Based on patent WO 9908189

Abstract (Basic): WO 9908189 A

Virus **signature** is created and written in form of Boolean expression using **signatures** of components as operands of Boolean expression. Processor scans data streams for components of virus, and scan results are used by processor to evaluate Boolean expression in order to determine existence of virus.

The processor receives (305) request from application executing on computer system to scan select files for viruses. Processor gets data streams comprising selected files retrieved from storage medium and stores them in system memory for identification (315) either as belonging to one file or several files, and scans (320) identified data streams for component of virus **signatures** to be written to system memory (330). Specifically for each virus **signature** , the processor scans the data **streams** for operands of Boolean expression that represents the virus **signature** . Preferably, **separate** scans are done for each file or for data **streams** belonging to several files Data streams of one file can be divided into several groups and scanned by group.

USE - For detecting computer viruses that span multiple data streams (CLAIMED).

ADVANTAGE - Is capable of identifying correctly virus components spanning multiple data streams, can create virus **signatures** and indicate presence of several components.

DRAWING DESCRIPTION - Drawing illustrates method of detecting computer viruses according to present invention, with self-explanatory flow diagram of process execution.

Dwg.3a/5

Title Terms: DETECT; METHOD; COMPUTER; VIRUS; SPAN; MULTIPLE; DATA; STREAM; PROCESSOR; SCAN; DATA; STREAM; COMPONENT; VIRUS; SCAN; RESULT; PROCESSOR; EVALUATE; BOOLEAN; EXPRESS; ORDER; DETERMINE; EXIST; VIRUS
Derwent Class: T01
International Patent Class (Main): **G06F-011/00 ; G06F-012/14**
File Segment: EPI

12/5/11 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012289822 **Image available**
WPI Acc No: 1999-095928/199908
XRPX Acc No: N99-069700

Hash **value method for using addresses in compacting systems - involves initially assigning object address as** hash **value and when compacting retaining original address as** hash **value**

Patent Assignee: SUN MICROSYSTEMS INC (SUNM)
Inventor: AGESEN O
Number of Countries: 020 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9900733	A1	19990107	WO 98US13623	A	19980630	199908	B
EP 993634	A1	20000419	EP 98933007	A	19980630	200024	
			WO 98US13623	A	19980630		
US 6105040	A	20000815	US 97885561	A	19970630	200041	
EP 1260901	A2	20021127	EP 98933007	A	19980630	200302	
			EP 200215479	A	19980630		
EP 993634	B1	20030312	EP 98933007	A	19980630	200319	
			WO 98US13623	A	19980630		
			EP 200215479	A	19980630		
DE 69812098	E	20030417	DE 612098	A	19980630	200333	
			EP 98933007	A	19980630		

Priority Applications (No Type Date): US 97885561 A 19970630
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9900733	A1	E	34	G06F-012/02	
Designated States (National): JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 993634	A1	E		G06F-012/02	Based on patent WO 9900733
Designated States (Regional): DE FR GB					
US 6105040	A			G06F-017/30	
EP 1260901	A2	E		G06F-009/44	Div ex application EP 98933007 Div ex patent EP 993634
Designated States (Regional): DE FR GB					
EP 993634	B1	E		G06F-012/02	Related to application EP 200215479 Related to patent EP 1260901 Based on patent WO 9900733
Designated States (Regional): DE FR GB					
[illegible]	E			G06F-012/02	Based on patent EP 993634 Based on patent WO 9900733

Abstract (Basic): WO 9900733 A

The computer system operates object based applications that create objects and later remove some of them during memory compaction. Objects are created in a dynamically used space (650) and given two flags (614,616) that are initially zero. The flags indicate that no **hash** value has been assigned and the object has not been moved. When a **hash** value is assigned, the current address of the object is used and a flag set (644).

When memory is compacted, e.g. objects removed (620), objects that have no **hash** value can be freely moved. Objects with **hash** values are moved, a new **hash** field with the previous address is added and another flag set to indicate the additional word.

ADVANTAGE - Allows for compacting **without** unnecessary **hash** value storage and inherently good **hash** value **distribution** .

Dwg.6a,6b/
6

Title Terms: **HASH** ; VALUE; METHOD; ADDRESS; COMPACT; SYSTEM; INITIAL; ASSIGN; OBJECT; ADDRESS; **HASH** ; VALUE; COMPACT; RETAIN; ORIGINAL; ADDRESS; **HASH** ; VALUE
Derwent Class: T01
International Patent Class (Main): **G06F-009/44** ; **G06F-012/02** ; G06F-017/30
File Segment: EPI

12/5/12 **(Item 11 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

009416092 **Image available**
WPI Acc No: 1993-109605/199313
XRPX Acc No: N93-083514

Message processing system using multiple processors - has message receiving processor collecting network protocol processing information into digest **and transmitting processor reading** digest

Patent Assignee: DIGITAL EQUIP CORP (DIGI)
Inventor: BRYANT S F; SEAMAN M J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5195181	A	19930316	US 92820299	A	19920110	199313	B

Priority Applications (No Type Date): US 92820299 A 19920110
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5195181	A		16	G06F-013/00	

Abstract (Basic): US 5195181 A

The scheme implements workload partitioning between **separate** receive and **transmit** processors. Each receiving processor collects, into a **digest** , information relating to network protocol processing of a particular message, obtained via sequential byte processing of the message at the time of reception of the message. The information placed into the **digest** is information that is necessary for the completion of the processing tasks to be performed by the processor of the transmitting line card.

The **digest** is passed to the transmit processor through a buffer exchange between the receive and transmit processors. The transmit processor reads the **digest** before processing of the related message for transmission and uses the information in the network protocol processing of the message.

USE/ADVANTAGE - In multiprocessor router.

Dwg.1/8

Title Terms: MESSAGE; PROCESS; SYSTEM; MULTIPLE; PROCESSOR; MESSAGE; RECEIVE; PROCESSOR; COLLECT; NETWORK; PROTOCOL; PROCESS; INFORMATION; **DIGEST** ; TRANSMIT; PROCESSOR; READ; **DIGEST**

Derwent Class: T01; W01

International Patent Class (Main): **G06F-013/00**

File Segment: EPI

12/5/13 **(Item 12 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

008899014 **Image available**

WPI Acc No: 1992-026283/199204

XRPX Acc No: N92-019974

Processing device with highly integrated memory self-test facilities - decodes generated signature **word at test sequence end for execution as normal instruction**

Patent Assignee: PHILIPS ELECTRONICS NV (PHIG); PHILIPS GLOEILAMPENFAB NV (PHIG); NORTH AMERICAN PHILIPS CORP (PHIG)

Inventor: BALTUS P G; LIGHART M M; LIGTHART M M

Number of Countries: 006 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 467448	A	19920122	EP 91201750	A	19910705	199204	B
US 5224103	A	19930629	US 90553039	A	19900716	199327	
EP 467448	A3	19930113	EP 91201750	A	19910705	199346	
EP 467448	B1	19970528	EP 91201750	A	19910705	199726	
DE 69126249	E	19970703	DE 626249	A	19910705	199732	
			EP 91201750	A	19910705		
JP 3091526	B2	20000925	JP 91172685	A	19910712	200051	

Priority Applications (No Type Date): US 90553039 A 19900716

Cited Patents: NoSR.Pub; 3.Jnl.Ref

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 467448	A				
Designated States (Regional): DE FR GB IT					
US 5224103	A		10	G06F-011/00	
EP 467448	B1	E	15	G06F-011/00	
Designated States (Regional): DE FR GB IT					
DE 69126249	E			G06F-011/00	Based on patent EP 467448
JP 3091526	B2		10	G11C-029/00	Previous Publ. patent JP 4255000

Abstract (Basic): EP 467448 A

The built-in program memory (14) stores data including program instructions for controlling a functional unit (20). A signal generator (18) combines data read from all memory locations during a memory test sequence initiated by an external control signal, to generate a **signature** word used for verification means. This is decoded at the test finish for execution as a normal program instruction so directly

determining the subse nt operation of the device. Any instruction can be encoded using a seed word in the **signature** generation.

The **signature** generator is formed during memory test sequence by temporary reconfiguration of at least part of the instruction decoder.

ADVANTAGE - Verification result can be communicated externally without the need for a dedicated data path. (13pp Dwg.No.1/5

Title Terms: PROCESS; DEVICE; HIGH; INTEGRATE; MEMORY; SELF; TEST; FACILITY ; DECODE; GENERATE; **SIGNATURE** ; WORD; TEST; SEQUENCE; END; EXECUTE; NORMAL; INSTRUCTION
Derwent Class: T01; U11; U13; U14
International Patent Class (Main): **G06F-011/00** ; G11C-029/00
International Patent Class (Additional): G01R-031/28; **G06F-011/08** ; **G06F-011/27** ; **G06F-012/16** ; H04B-017/00
File Segment: EPI

12/5/14 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

05476 **Image available**
WPI Acc No: 1990-092477/199013
XRPX Acc No: N90-071402

Fault tolerant operation of multiprocessor systems - has signature **vectors generated by each processor for comparison to identify fault**

Patent Assignee: AKAD WISSENSCHAFTEN DDR (DEAK)
Inventor: STOPP A
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 3930075	A	19900322	DE 3930075	A	19890909	199013	B
DD 275545	A	19900124				199027	

Priority Applications (No Type Date): DD 319880 A 19880916
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 3930075	A		12		

Abstract (Basic): DE 3930075 A

A fault tolerant multiprocessor system is based upon a number of identical processors, each one of which has a CPU (1), ROM (4), RAM (5), timer (6), I/O interface (12) and a **communication** interface (11). Each of the processors has an error **independent signature** switching circuit (10) that are hierarchically connected to the highest priority processor.

The **signature** circuit operates to provide automatic monitoring of the processor, combined with testing and isolation of the unit in the event of a fault being identified. In association with the processor, the **signature** controls a cycle that results in fault correction. The control algorithm is based upon comparison of **signature** values.

ADVANTAGE - Provides high fault-tolerant mode of operation

Title Terms: FAULT; TOLERATE; OPERATE; MULTIPROCESSOR; SYSTEM; **SIGNATURE** ; VECTOR; GENERATE; PROCESSOR; COMPARE; IDENTIFY; FAULT
Derwent Class: T01
International Patent Class (Additional): **G06F-011/16**
File Segment: EPI

File 348:EUROPEAN PATENTS 1978-2004/Feb W01
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040205,UT=20040129
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	49572	SIGNATURE? ? OR HASH?? OR DIGEST? ?
S2	1082462	SEPARATE OR SEPARATELY OR INDEPENDENT? OR DETACHED OR UNATTACHED OR (DE OR UN)()ATTACHED OR DISCONNECTED OR ISOLATED OR APART()"FROM"
S3	1090644	WITHOUT OR BY()ITSELF OR ("NOT" OR T)(1W)(INCLUD? OR ATTACH? OR WITH OR CONNECT? OR DEPENDENT?)
S4	386	S1(5N)S2:S3(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSION OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BROADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COMMUNICAT? OR FORWARD?)
S5	2	S4 AND IC=G09C
S6	111	S4 AND IC=H04L
S7	129	S4 AND IC=G06F
S8	26	S6 AND S7
S9	214	S6:S7
S10	187	S9 NOT (S5 OR S8)
S11	24	S10/TI,AB,CM
S12	163	S10 NOT S11
S13	118	SIGNATURE(5N)S2(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSION OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BROADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COMMUNICAT? OR FORWARD?)
S14	89	S13 AND S12
???	55	S13 NOT (S5 OR S8 OR S11 OR S14)

14/3,K/33 (Item 21 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00769798 **Image available**
SYSTEM AND METHODS FOR PROVING DATES IN DIGITAL DATA FILES
SYSTEME ET PROCEDES PERMETTANT D'ATTRIBUER DES DATES A DES FICHIERS DE DONNEES NUMERIQUES
Patent Applicant/Assignee:
TIMF CERTAIN LLC, 7041 Western Avenue, Washington, DC 20015, US, US (Residence), US (Nationality)
Inventor(s):
TRITTER Steven W, 7401 Western Avenue, Washington, DC, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200103363 A1 20010111 (WO 0103363)
Application: WO 2000US18259 20000630 (PCT/WO US0018259)
Priority Application: US 99142132 19990702; US 99429360 19991028
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 26468

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... data element 180 is, in some cases as will be described in greater detail herein below, referred to as a "digital certificate". Furthermore, the digital **signature** 160 may be simply **transmitted** or stored as a **separate** data element, so long as it maintains a reliable association with its message I 1 0. Each digital signature 160 is unique to the ...

14/3,K/34 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00749027 **Image available**
UNIVERSAL SYNCHRONOUS NETWORK SYSTEM FOR INTERNET PROCESSOR AND WEB OPERATING ENVIRONMENT
SYSTEME DE RESEAU SYNCHRONE UNIVERSEL POUR PROCESSEUR INTERNET ET ENVIRONNEMENT DE FONCTIONNEMENT INTERNET
Patent Applicant/Assignee:
STANFORD SYNCOM INC, 2390 Walsh Avenue, Santa Clara, CA 95051, US, US (Residence), US (Nationality)
Inventor(s):
TRANS Francois, 1504 Clay Drive, Los Altos, CA 94024, US
Legal Representative:
MCNELIS John T, Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200062470 A1 20001019 (WO 0062470)
Application: WO 2000US10101 20000414 (PCT/WO US0010101)
Priority Application: US 99129314 19990414; US 99417528 19991013; US 99444007 19991119; US 99170455 19991213; WO 68US42 20000315
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK FI FR GB GR IE IT LU MC NL PT
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 97387

Main International Patent Class: **H04L-007/00**
Fulltext Availability:
Detailed Description

Detailed Description
... waveforms. The security system transmits the signature of the waveform by pre-positioning the signal at a specific frequency and phase matrix cell. The signal **signature** of the wavefonn's content is provided

14/3,K/35 (Item 23 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00122209 **Image available**
RELIANCE MANAGER FOR ELECTRONIC TRANSACTION SYSTEM
GESTIONNAIRE DE FIABILITE POUR SYSTEME DE TRANSACTIONS ELECTRONIQUES
Patent Applicant/Inventor:
FRANKEL Yair, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
MONTGOMERY Charles T, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
STUBBLEBINE Stuart, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
YUNG Marcel Mordechay, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), IL (Nationality), (Designated only for: US)
ANKNEY Richard, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
SALZ Richard, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
TITCHENER Thomas, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
LIEBERWIRTH Peter, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
KONSTANTARAS Andrew, Suite 22, 55 Broad Street, New York, NY 10004, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
LAZAR Dale S, Pillsbury Madison & Sutro, LLP, 1100 New York Avenue, N.W., Washington, DC 20005, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200045564 A1 20000803 (WO 0045564)
Application: WO 2000US2013 20000128 (PCT/WO US0002013)
Priority Application: US 99118379 19990129
Designated States: AU CA JP US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 29681

Main International Patent Class: **H04L-029/06**
Fulltext Availability:
Detailed Description

Detailed Description
... or whether the Relying Party wishes to accept the Signing Party offer to purchase the warranty (reqType is "ACCEPT").
The signer's certificate chain is **conveyed** in the **detached signature**, rather
than as a **separate** XML element. The **detached signature** consists of the

SignerInfo structure, a [redacted]rsion number, **digest** algorith[redacted]ID, and (optionally) certificates.

1 0 The relying party may include the entire signed transaction rather than the detached signature. This would be the...

...and the time for which the offer is valid.

CUSTOMER OFFER (XML)
1 0 The Relying Party Bank creates a CMS SignedData message containing the **detached signature** of the original transaction and the offer. The **forwarded**
fier is identical in syntax to the interbank offer
EMENT customer-offer
id, amount, expires, fee, offer-expires) >
ITANCE (XML)
The Relying Party creates a...

14/3,K/36 **(Item 24 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT

00731926 **Image available**
METHOD AND SYSTEM FOR DYNAMIC CONFIGURATION OF INTERCEPTORS IN A CLIENT-SERVER ENVIRONMENT
PROCEDE ET SYSTEME DE CONFIGURATION DYNAMIQUE D'INTERCEPTEURS DANS UN ENVIRONNEMENT DE SERVEUR CLIENT
Patent Applicant/Assignee:
IONA TECHNOLOGIES INC, 200 West Street, Waltham, MA 02451, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KUKURA Robert A, 200 West Street, Waltham, MA 02451, US, US (Residence), US (Nationality), (Designated only for: US)
RYAN Craig, 200 West Street, Waltham, MA 02451, US, US (Residence), US (Nationality), (Designated only for: US)
MIHIC Matthew A, 200 West Street, Waltham, MA 02451, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
REIN Barry D (et al) (agent), Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200045256 A1 20000803 (WO 0045256)
Application: WO 2000US2189 20000128 (PCT/WO US0002189)
Priority Application: US 99117938 19990129; US 99117950 19990129; US 99117946 19990129; US 99117944 19990129
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 28537

Main International Patent Class: **G06F-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... into the CORBA module so that may become usable on CORBA module stubs.

.. should also be noted that if the request is not time- **independent** ,
...
transport interceptor needs to remember the **signature** so that it can

convert the response to [redacted] an invocation on the ReplyHan[redacted]er. The ART core might provide some assistance in this aspect...

14/3,K/37 (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

[illegible]2 **Image available**
METHOD AND APPARATUS FOR MULTIPLEXING SEPARATELY-AUTHORED METADATA FOR INSERTION INTO A VIDEO DATA STREAM
PROCEDE ET APPAREIL DE MULTIPLEXAGE DE METADONNEES MEDIATISEES SEPAREMENT POUR INSERTION DANS UN FLUX DE DONNEES VIDEO
Patent Applicant/Assignee:
HOTV INC, 12625 High Bluff Drive, #315, San Diego, CA 92130, US, US (Residence), US (Nationality)
Inventor(s):
SRINIVASAN Anand, 12718 Torrey Bluff Drive, #155, San Diego, CA 92130, US
SHAH Mehul Y, 12633 El Camino Real #3408, San Diego, CA 92130, US
CHAKRABORTY Indranil, 12633 El Camino Real #3408, San Diego, CA 92130, US
MARDIKAR Mohan, 12640 Torrey Bluff Drive, #7, San Diego, CA 92130, US
RANGAN P Venkat, 13011 Callcott Way, San Diego, CA 92130, US
BHADADA Kamal, 12782 Torrey Bluff Drive #103, San Diego, CA 92130, US
Legal Representative:
BOYS Donald R, P.O. Box 187, Aromas, CA 95004, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200043899 A1 20000727 (WO 0043899)
Application: WO 2000US1699 20000121 (PCT/WO US0001699)
Priority Application: US 99235781 19990122
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 24983

Main International Patent Class: **G06F-015/167**
Fulltext Availability:
Detailed Description

Detailed Description
... deliver separate streams via separate carriers to an end user. Also known to the inventor is a system for providing a means of applying a **signature** and associative frame identification to the **separate streams** respectively before **broadcast** so that both streams may later be resynchronized at the user's end. Such a system is likewise described under the crossreferencing section.

In current...wherein an arriving video feed is recorded digitally and edited before re-broadcast.

It must also be noted here that in a case of sending **separate streams** (one video and one annotation) via **separate** media, the **signature** process as described with
reference to the section entitled Method and Apparatus for Combining and Synchronizing Separately Sourced Video-Stream Data must be applied after ...

14/3,K/38 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00559414 **Image available**
METHOD, SYSTEM, AND COMPUTER PROGRAM PRODUCT FOR PROVIDING ENHANCED ELECTRONIC MAIL SERVICES
PROCEDE, SYSTEME ET PRODUIT DE PROGRAMME INFORMATIQUE POUR DES SERVICES DE COURRIER ELECTRONIQUE RENFORCES
Patent Applicant/Assignee:
BANKERS TRUST COMPANY,
Inventor(s):
SUDIA Frank Wells,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200022787 A2 20000420 (WO 0022787)
Application: WO 99US23453 19991008 (PCT/WO US9923453)
Priority Application: US 98168936 19981009
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 24338
Main International Patent Class: **H04L-012/58**
International Patent Class: **H04L-029/06** ...

... **H04L-009/32** ...

... **H04L-009/08**
Fulltext Availability:
Detailed Description

Detailed Description
... been added to this embodiment of the protocol, as shown in Table 5. First, the signature of A, SA, over MO is enhanced to include **signature** attributes, which are **delivered** along with the **signature** block, containing **separate** **hash** values for: (1) H(M) - placing the **hash** of the inner content, M, into the signature links A to M in the eyes of both B and the PO 240; 5 (2) H...M using K MO = Epo(A I B I MB X
A -4 B: M,,
B: R = SB(MO
B -4 A: R Preferably a **detached** **signature**
A: verify R
A -4 B: MO I X **Send** MB per basic version, along with
... Kp. and "A I B I MB X" Info to
... MO
Verify MO same...

14/3,K/39 **(Item 27 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00476837
DETECTION OF COMPUTER VIRUSES SPANNING MULTIPLE DATA STREAMS
DETECTION DE VIRUS INFORMATIQUES DISSEMINES DANS PLUSIEURS TRAINS DE DONNEES
Patent Applicant/Assignee:
SYMANTEC CORPORATION,
Inventor(s):
CHI Darren,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9908189 A1 19990218
Application: WO 98US13774 19980630 (PCT/WO US9813774)
Priority Application: US 97909203 19970811
Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English

Fulltext Word Count: 6693

Main International Patent Class: **G06F-011/00**
Fulltext Availability:
Detailed Description
Detailed Description
... Traditionally, the entire body of a virus has been wholly contained within one data stream. As a result, current virus detection technologies ... data **stream** for an entire virus **signature** and examine each ... **stream** for viruses **independently** of other data **streams** .

... developed operating systems and file formats include data entities that are a collection of data streams. Examples of these entities are Apple Macintosh files...each component resides in a different data stream, each of the first three viruses spans two data streams and the fourth virus spans three data **streams** . Scanning each data **stream** **independently** of other data **streams** for the entire virus **signature** of any of these viruses will not result in any of the viruses being detected. ...the other viruses, to the virus B/P 1. Therefore, if the probability is low that the component B will be found in scanned data **streams** **without** the virus B/P I contaminating the data **streams** , the **signature** for the virus B/P I is the signature for component B (Component Sig/B). If the probability is not low that component B will...

...more components that is unique to the virus, the signature creator determines 245 whether the probability is low that the combination will exist in data **streams** **without** the virus existing. If the probability is low, the **signature** for the combination, which is logically in the form of a Boolean expression, is used as the signature for the whole virus (step 250). For...

14/3,K/40 **(Item 28 from file: 349)**
... File 349:PCT FULLTEXT
... WIPO/Univentio. All rts. reserv.

... All
BIOMETRIC CERTIFICATES
CERTIFICATS BIOMETRIQUES
Patent Applicant/Assignee:
GTE GOVERNMENT SYSTEMS CORPORATION,
GTE SERVICE CORPORATION,
Inventor(s):
DULUDE Robert,
MUSGRAVE Clyde,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9850875 A2 19981112
Application: WO 98US9770 19980508 (PCT/WO US9809770)
Priority Application: US 9746012 19970509
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 5634
...International Patent Class: **H04L-009/28** ...

... **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... sent to the network
6 0 .

The set of data transmi. ons constituting the transacti
biometric data 46, the transaction first data 50, and the
digital **signature** 58 may be **sent** as **separate** bitstreams and/or
data packets, or otherwise may be sent together by appending
the associated data sequences using a concatenator, such as an
adder...

14/3,K/41 (Item 29 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00430181 **Image available**
IMPROVED TRI-SIGNATURE SECURITY ARCHITECTURE SYSTEMS AND METHODS
SYSTEMES ET PROCEDES AMELIORES D'ARCHITECTURE DE SECURITE A TRIPLE SIGNATURE
Patent Applicant/Assignee:
TRI-STRATA SECURITY INC,
Inventor(s):
ATALLA Martin M,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9820645 A2 19980514
Application: WO 97US19310 19971103 (PCT/WO US9719310)
Priority Application: US 96740946 19961105
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES
FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN
MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW
GH KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI
FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 8745

Main International Patent Class: **H04L-009/08**
Fulltext Availability:
Detailed Description

Detailed Description
... compartment contains N bytes, the maximum number of key streams based upon a single pointer using sequential addresses to identify the bytes in each session **signature** is N. This o number is **independent** of the **stream** length desired. For n compartments, the maximum number of streams is Nn-1. Thus for four compartments each containing one million bytes, the maximum number of this invention, random pointers to different session **signatures** and a master **signature** can be used to obtain two **separate** key **streams** for full duplex (i.e. two way or bidirectional) operation. Each key stream can be derived as described in any of the ways above. In...N key
2 5 stream segments each up to N bytes long from two randomly selected compartments each containing N bytes selected from a master **signature** .

Figure 9 shows a duplex key **stream** where two **separate** key **streams** A and
B are derived from the same master **signature** , each key **stream** though being **independent** of the other key **stream** .
8
Figure 1 0 shows the shared key bucket and DES key bucket embodiment where the DES key resides only in the security server and...

14/3,K/42 (Item 30 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00384143 **Image available**
COMMUNICATIONS SYSTEM AND METHOD PROVIDING OPTIMAL RESTORATON OF FAILED PATHS
SYSTEME ET PROCEDE DE COMMUNICATION DONNANT UNE RESTAURATION OPTIMALE DES

CHEMINS DEFECTUEUX
Patent Applicant/Assignee:
MCI COMMUNICATIONS CORPORATION,
Inventor(s):
ALLEN John David,
BENGSTON Lee D,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9724886 A1 19970710
Application: WO 96US20143 19961230 (PCT/WO US9620143)
Priority Application: US 95580718 19951229
Designated States: CA JP MX AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT
Publication Language: English
Fulltext Word Count: 9788

International Patent Class: **H04L-12:56**
Fulltext Availability:
Detailed Description

Detailed Description
... is already assigned to the port by the action of the same node functioning as a Sender or a Tandem in the context of a **separate** restoration process.

Each **signature** in the **transmit** queue has an associated HOLD FLAG, which indicates whether the signature is eligible for retransmission at a later time.

As will be explained in FIGS...

14/3,K/43 (Item 31 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00376159
UNIFIED END-TO-END SECURITY METHODS AND SYSTEMS FOR OPERATING ON INSECURE NETWORKS
PROCEDES ET SYSTEMES UNIFIES PRESENTANT UNE SECURITE DE BOUT EN BOUT ET SERVANT A UNE EXPLOITATION SUR DES RESEAUX NON SURS
Patent Applicant/Assignee:
TRI-STRATA SECURITY INC,
Inventor(s):
ATALLA Martin M,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9716902 A2 19970509
Application: WO 96US17479 19961101 (PCT/WO US9617479)
Priority Application: US 9529 19951102
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 23564
Main International Patent Class: **H04L-009/08**
Fulltext Availability:
Detailed Description

Detailed Description
... using a split signature procedure.

Figure 5 shows the relationship between a user, an insecure network and multiple network computers, each network computer having a **separate** access **signature** for **communicating** with the user, all access **signatures** being selected randomly from the same master signature of the user.

Figure 6 shows a symmetric mode of operation where two network computers, each with...master signature, the addresses of the access signature residing at network computer 12. Each side, now, is made equally responsible for generating one of two **separate** parts of the session **signature** : each side **transmits** to the other the addresses only of the part of the session signature that it has generated. upon completion of this transmission from each side...same as in conjunction with Figure 4A.

Figure 5 illustrates the operation of this invention in the asymmetric mode wherein one user with one master **signature** is able to **communicate** with multiple computers each having a **separate** access **signature** all randomly selected from the one master **signature** of the user. As shown in Figure 5, the user at terminal 50 has an I.D. as well as a master signature. The master...a particulr user from captured transmitted information, this alternative embodiment makes it even more difficult, if not impossible. Simply, it does not allow even the **signature** addresses to be **transmitted** **without** prior encryption. This alternative embodiment makes it even more practical to use simplified and more efficient security procedures and to utilize extremely simple and fast...

14/3,K/44 **(Item 32 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00352939 **Image available**
SYSTEM AND METHOD FOR RESOLVING SUBSTANTIALLY SIMULTANEOUS BI-DIRECTIONAL REQUESTS OF SPARE CAPACITY
SYSTEME ET PROCEDE VISANT A RESOUDRE LES DEMANDES BIDIRECTIONNELLES PRATIQUEMENT SIMULTANEES DE CAPACITE DISPONIBLE
Patent Applicant/Assignee:
MCI COMMUNICATIONS CORPORATION,
Inventor(s):
WILL Russ,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9641453 A1 19961219
Application: WO 96US10491 19960607 (PCT/WO US9610491)
Priority Application: US 95483578 19950607
Designated States: CA JP MX AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 5966

Main International Patent Class: **H04L-012/407**
Fulltext Availability:
Detailed Description

Detailed Description
... substantially the same time that a flooding signature was sent by node 6 into the same link. Since node 5 is performing its own arbitration **independently** of that being performed by node 6, assume the flooding **signature** **sent** out by node 5 would have reached node 6 by the end of

14/3,K/45 **(Item 33 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00357251

MULTI-STEP DIGITAL SIGNATURE METHOD AND SYSTEM
PROCEDE ET SYSTEME DE SIGNATURE NUMERIQUE A ETAPES MULTIPLES
Patent Applicant/Assignee:
  BANKERS TRUST COMPANY,
  SUDIA Frank W,
  FREUND Peter C,
  HUANG Stuart T F,
Inventor(s):
  SUDIA Frank W,
  FREUND Peter C,
  HUANG Stuart T F,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9639765 A1 19961212
  Application: WO 96US5317 19960419 (PCT/WO US9605317)
  Priority Application: US 95462430 19950605
Designated States: AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB
  GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL
  PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN KE LS MW SD SZ UG AM
  AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT
  SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 16280

Main International Patent Class: **H04L-009/30**
International Patent Class: **H04L-09:32**
Fulltext Availability:
  Detailed Description

Detailed Description
... three or more factors. Unless stated
  otherwise, all arithmetic operations are to be considered
  modulo N

  In the multi-step signature method, shares of a
  signature key a1, a2, ... ab o are **distributed** to **separate**
  devices. A first device affixes a partial **signature** to a
  document by hashing the document (the symbol "H" will be used
  to designate the result of the hash operation) and
  exponentiating the hash...

14/3,K/46 **(Item 34 from file: 349)**
[Also in File 349:PCT FULLTEXT]

00330504 **Image available**
MULTI-STAGE PARCEL TRACKING SYSTEM
SYSTEME DE SUIVI DE COLIS MULTIPHASE
Patent Applicant/Assignee:
  UNITED PARCEL SERVICE OF AMERICA INC, 55 Glenlake Parkway, N.E., Atlanta,
    GA 30328, US, US (Residence), US (Nationality)
Inventor(s):
  KADABA Nagesh, 5 Hearthstone Drive, Brookfield, CT 06804, US,
  MOKTAN Hridai, 14 Chatham Court, Brookfield, CT 06804, US,
  PATEL Mark, Apartment No. 8, 1 Luffberry Avenue, Norwalk, CT 06851, US,
Legal Representative:
  PAPPAS Peter G (et al) (agent), Jones & Askew, 37th floor, 191 Peachtree
    Street, N.E., Atlanta, GA 30303-1769, US,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9613015 A2-A3 19960502
  Application: WO 95US13203 19951013 (PCT/WO US9513203)
  Priority Application: US 94323118 19941014
Designated States: CA JP
  (EP) AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 6120

Main International Patent ass: **G06F-017/60**
Fulltext Availability:
Detailed Description

Detailed Description
... recipient, the user has the ability to scan the parcel bar code or enter the recipient's employee number, and to capture the recipient's **signature** . No **separate** stylus is required for screen data entry. **Delivery** information query management allows the user to obtain tracking information by date, by tracking number, or by employee name or number or location. Communication by...

14/3,K/47 (Item 35 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00320485
METHOD FOR SECURELY USING DIGITAL SIGNATURES IN A COMMERCIAL CRYPTOGRAPHIC SYSTEM
PROCEDE PERMETTANT D'UTILISER EN TOUTE SECURITE DES SIGNATURES NUMERIQUES DANS UN SYSTEME DE CHIFFRAGE COMMERCIAL
Current Applicant/Assignee:
BANKERS TRUST COMPANY,
SUDIA Frank W,
SIRITZKY Brian,
Inventor(s):
SUDIA Frank W,
SIRITZKY Brian,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9602993 A2 19960201
Application: WO 95US9076 19950719 (PCT/WO US9509076)
Priority Application: US 94277438 19940719
Designated States: AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TT UA UG US UZ VN KE MW SD SZ UG AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 14898

Main International Patent Class: **H04L-009/32**
Fulltext Availability:
Detailed Description

Detailed Description
... with biometric techniques. This WO 96/02993 PCTIUS95/09076 completeness in order to round out the "relative identity" concept,
Authorization Informgtion in Certificates
Attributes may **convey** restrictions that control the conditions under which a **signature** is valid.

Without such restrictions, the risk of forgery would be considered excessive, since an electronic signature can be affixed to almost any digital document by anyone possessing...signature capabilities already assumed can be expanded to provide a framework for this service.

For notarization purposes, timestamps and location information will be included as **signature** attributes. Individual **signature** structures may either be **detached** and stored or, if desired, **conveyed separately** from the document.

Multiple **signatures** or joint **signatures** on the document itself can also be distinguished from

"countersignatures," wh are signatures on the signature structure in which they are found and not on...

14/3,K/48 (Item 36 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00205806 **Image available**
METHOD FOR SECURE TIME-STAMPING OF DIGITAL DOCUMENTS
PROCEDE D'HORODATAGE SUR DE DOCUMENTS NUMERIQUES
Patent Applicant/Assignee:
BELL COMMUNICATIONS RESEARCH INC,
Inventor(s):
HABER Stuart Alan,
STORNETTA Wakefield Scott Jr,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9203000 A1 19920220
Application: WO 91US5386 19910730 (PCT/WO US9105386)
Priority Application: US 90888 19900802; US 91896 19910308
Designated States: AT BE CA CH DE DK ES FR GB GR IT JP LU NL SE
Publication Language: English
Fulltext Word Count: 6915

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... proceeds as previously indicated with the exception that each agent individually adds the current time data to the representative document it receives, certifies the resulting **separate** time-stamped receipt with its own verifiable cryptographic **signature** , and **transmits** the certificate back to the author. This transmittal may be directly to the requesting author or by way of the administrative TSA where the receipts...

```
File   8:Ei Compendex(R)     0-2004/Feb W1
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Jan
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Jan 20
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Feb W2
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Feb W1
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Feb W1
         (c)2004 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2004/Feb W2
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/Feb W1
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Feb W2
         (c) 2004 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Jan
         (c) 2004 The HW Wilson Co.
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 266:FEDRIP 2004/Dec
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2004/Jan W4
         (c) 2004 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2004/Jan
         (c) 2004 The HW Wilson Co

Set     Items   Description
S1     172606   SIGNATURE? ? OR HASH?? OR DIGEST? ?
S2    2544254   SEPARATE OR SEPARATELY OR INDEPENDENT? OR DETACHED OR UNAT-
                TACHED OR (DE OR UN)()ATTACHED OR DISCONNECTED OR ISOLATED OR
                APART()"FROM"
S3    1911385   WITHOUT OR BY()ITSELF OR ("NOT" OR T)(1W)(INCLUD? OR ATTAC-
                H? OR WITH OR CONNECT? OR DEPENDENT?)
S4        131   S1(5N)S2:S3(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSI-
                ON OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BRO-
                ADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COM-
                MUNICAT? OR FORWARD?)
S5         83   RD (unique items)
S6         59   S5 NOT PY=2000:2004
S7          8   S6 AND DIGITAL()SIGNATURE? ?
S8         51   S6 NOT S7
```

7/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03866645 E.I. No: EIP94051299310
Title: Subliminal channels for transferring signatures: Yet another cryptographic primitive
Author: Sakurai, Kouichi; Itoh, Toshiya
Corporate Source: Mitsubishi Electric Corp, Kamakura-shi, Jpn
Source: IEICE Transactions on Fundamentals of Electronics, Communicationsand Computer Sciences v E77-A n 1 Jan 1994. p 31-38
Publication Year: 1994
CODEN: IFESEX ISSN: 0916-8508
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review); T; (Theoretical)
Journal Announcement: 9407W2
Abstract: This paper considers the subliminal channel, hidden in an identification scheme, for transferring signatures. We observe the direct parallelization of the Fiat-Shamir identification scheme has a subliminal channel for the transmission of the **digital signature** . A positive aspect of this hidden channel supplies us how to **transfer signatures without** secure channels. As a formulation of such application, we introduce a new notion called privately recordable signature. The privately recordable signature is generated in an interactive protocol between a signer and a verifier, and only the verifier can keep the signatures although no third adversary can record the signatures. In this scheme, then the disclosure of the verifier's private coin turns the signer's signature into the ordinary **digital signature** which is verified by anybody with the singer's public key. The basic idea of our construction suggests the novel primitive that a **transferring** securely **signatures without** secret channels could be constructed using only one-way function (**without** trapdoor). (Author abstract) 47 Refs.
Descriptors: *Cryptography; Communication channels (information theory); Classification (of information); Data processing; Data handling; Security of data; Network protocols; Theorem proving
Identifiers: Subliminal channels; Privately recordable signature; **Digital signatures** ; Fiat Shamir scheme
Classification Codes:
723.2 (Data Processing); 716.1 (Information & Communication Theory); 903.1 (Information Sources & Analysis); 723.1 (Computer Programming); 722.3 (Data Communication, Equipment & Techniques); 721.1 (Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory)
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment); 903 (Information Science); 722 (Computer Hardware); 721 (Computer Circuits & Logic Elements)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 90 (GENERAL ENGINEERING)

7/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01745411 E.I. Monthly No: EI8504026318 E.I. Yearly No: EI85029318
Title: FAST AND SECURE DIGITAL SIGNATURE USING PUBLIC-KEY CRYPTOSYSTEMS.
Author: Koyama, Kenji
Corporate Source: NTT, Musashino Electrical Communication Lab, Musashino, Jpn
Source: Systems - Computers - Controls v 15 n 5 Sep-Oct 1984 p 1-10
Publication Year: 1984
CODEN: SYCCBB ISSN: 0096-8765 ISBN: 0-8243-0717-8
Language: ENGLISH
Document Type: JA; (Journal Article) Treatment: A; (Applications); T; (Theoretical)
Journal Announcement: 8504

Abstract: Existing **digital signature** systems are the viewpoints of encryption, check method and construction, are classified by describing their features and problems. Semantic processing in message recovery method is discussed, which is a check method for the true signature. It is shown based on entropy that, in order to determine whether or not the recovered message is meaningful, the message length must be equal to or larger than the unicity distance. It is also shown that decision by semantic processing is impossible in principle for a message with zero redundancy. Merits and demerits of adding such information as the data to the message are discussed. As a system which an essentially solve semantic processing problem **without** requiring the **delivery** of the secret key, an improved **digital signature** method is proposed which combines a message recovery method using the public-key cryptosystem and an authenticator verification method using the public-key cryptosystem. 12 refs.

Descriptors: *DATA PROCESSING--*Security of Data; INFORMATION SCIENCE

Identifiers: **DIGITAL SIGNATURE** ; PUBLIC-KEY CRYPTOSYSTEMS; SEMANTIC PROCESSING; MESSAGE RECOVERY METHOD; AUTHENTICATION VERIFICATION

Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

7/5/3 **(Item 1 from file: 35)**
DIALOG(R)File 35:Dissertation Abs Online

914277 ORDER NO: AAD86-07344
DESIGNING FAULT-TOLERANT ALGORITHMS FOR DISTRIBUTED SYSTEMS USING COMMUNICATION PRIMITIVES (BYZANTINE, AGREEMENT)

Author: SRIKANTH, T. K.
Degree: PH.D.
Year: 1986
Corporate Source/Institution: CORNELL UNIVERSITY (0058)
Source: VOLUME 47/02-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 699. 114 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984

Fault-tolerance is an important requirement in distributed computing systems. However, designing applications for distributed systems is a difficult task, particularly when components of the system can fail. The difficulty of this task increases with the severity of failures encountered. Arbitrary process failures are generally much harder to overcome than failures that are restricted, e.g., where processes only fail by halting. Thus, techniques that restrict the disruptive behavior of faulty processes can greatly simplify the design of fault-tolerant algorithms. Such techniques effectively provide reduction mechanisms from one class of failures to a more benign class.

Message authentication is an example of a technique that imposes restrictions on the externally visible behavior of faulty processes. This technique has been used to derive simple solutions to many problems of fault-tolerance for systems with arbitary faults. To exploit the simplicity provided by authentication, we present **communication** primitives that provide properties of authentication **without** using **digital signatures** . These primitives can also be extended to provide properties beyond those of authentication, thereby further restricting the types of faults that have to be overcome.

These communication primitives lead to a general methodology for designing fault-tolerant algorithms. We first design an algorithm assuming that messages are signed. Then, replacing signed communication in this algorithm with our broadcast primitive automatically results in an equivalent non-authenticated algorithm. We illustrate this methodology by presenting new solutions to the problems of distributed agreement and clock synchronization in the presence of faults. Our solutions to the problems of Byzantine Agreement, early-stopping Byzantine Agreement, Byzantine Elections, and clock synchronization are simpler and more efficient than those previously known. Furthermore, the clock synchronization algorithm that we propose is the first one that achieves optimal accuracy with

respect to real time.

7/5/4 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

4578011 INSPEC Abstract Number: B9402-6120B-122, C9402-6130S-076
Title: Subliminal channels for signature transfer and their application to signature distribution schemes
Author(s): Sakurai, K.; Itoh, T.
Author Affiliation: Comput. & Inf. Syst. Lab., Mitsubishi Electr. Corp., Kamakura, Japan
Conference Title: Advances in Cryptology - AUSCRYPT '92. Workshop on the Theory and Application of Cryptographic Techniques Proceedings p.231-43
Editor(s): Seberry, J.; Zheng, Y.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1993 Country of Publication: West Germany xiii+542 pp.
ISBN: 3 540 57220 1
Conference Date: 13-16 Dec. 1992 Conference Location: Gold Coast, Qld., Australia
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: The direct parallelization of the Fiat-Shamir identification scheme has a subliminal channel for transmission of the **digital signature**, which does not exist in the serial (zero-knowledge) version. This channel is applied to a multi-verifier interactive protocol and a **distributed** verification **signature** is proposed that cannot be verified **without** all verifiers' co-operation. The basic idea of construction suggests the novel primitive with which a signature transfer secure against an adversary can be constructed using only a one-way function (without trapdoor). (36 Refs)
Subfile: B C
Descriptors: cryptography; protocols; telecommunication channels
Identifiers: signature transfer; signature distribution schemes; Fiat-Shamir identification scheme; subliminal channel; multi-verifier interactive protocol; distributed verification signature; primitive; one-way function
Class Codes: B6120B (Codes); B6150M (Protocols); C6130S (Data security); C5640 (Protocols)

7/5/5 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

03789443 INSPEC Abstract Number: B91003821, C91004287
Title: Showing credentials without **identification**: transferring signatures **between unconditionally unlinkable pseudonyms**
Author(s): Chaum, D.
Conference Title: Advances in Cryptology-AUSCRYPT '90 International Conference on Cryptology. Proceedings p.246-64
Editor(s): Seberry, J.; Pieprzyk, J.
Publisher: Springer-Verlag, Berlin, West Germany
Publication Date: 1990 Country of Publication: West Germany ix+462 pp.
ISBN: 3 540 53000 2
Conference Date: 8-11 Jan. 1990 Conference Location: Sydney, NSW, Australia
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Theoretical (T)
Abstract: Different approaches to automating interactions yield quite different results. One extreme approach requires individuals always to show universal identifiers. The opposite extreme approach to automating relationships is complete anonymity. These extreme alternatives would make verifiability by organizations or control by individuals mutually

exclusive. The solution presented in this paper, however, offers the best of both worlds. Information transfer between relationships is controlled by individuals-yet transfers are incontestable. Two assumptions are made initially and relaxed later. The first, in the context of fixed sets of individuals and organizations, allows each individual at most one relationship per organization. Every such relationship is carried out under a unique 'account number' called a digital pseudonym. The items of information that an individual transfers between these pseudonymous relationships are called credentials. The second assumption is that only a particular organization, called Z, has the power to create pseudonyms or to issue credentials; nevertheless, Z learns no more about a person than do other organizations. The basic concept is introduced by analogy and then the actual system using **digital signatures** is explained. How pseudonyms are authorized is then detailed. After relaxing the two assumptions, the author illustrates the result with several applications. With the presented protocols, individuals can transform one credential into another and obtain new credentials by combining and making choices among those they already have. Finally, building on these techniques the author achieves the quite general result of allowing people exclusive control over the database of all their own relationships. (0 Refs)

Subfile: B C

Descriptors: cryptography; data privacy; protocols

Identifiers: interaction automation; individual control; signature transfer; incontestable transfers; authorization; zero knowledge protocols; credentials; unconditionally unlinkable pseudonyms; identifiers; anonymity; verifiability; account number; digital pseudonym; **digital signatures** ; database

Class Codes: B6120B (Codes); B6150 (Communication switching theory); C6130 (Data handling techniques)

7/5/6 (Item 3 from file: 2)

03158227 INSPEC Abstract Number: B88040838, C88033347

Title: A high speed manipulation detection code

Author(s): Jueneman, R.R.

Author Affiliation: Comput. Scis. Corp., Falls Church, VA, USA

Conference Title: Advances in Cryptology - CRYPTO '86 Proceedings p. 327-46

Editor(s): Odlyzko, A.M.

Publisher: Springer-Verlag, Berlin, West Germany

Publication Date: 1987 Country of Publication: West Germany xi+487 pp.

ISBN: 3 540 18047 8

Conference Sponsor: Int. Assoc. Cryptologic Res.; IEEE

Conference Date: 11-15 Aug. 1986 Conference Location: Santa Barbara, CA, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: Manipulation detection codes (MDC) are defined as a class of checksum algorithms which can detect both accidental and malicious modifications of an electronic message or document. Although the MDC result must be protected by encryption to prevent an attacker from succeeding in substituting his own manipulation detection code (MDC) along with the modified text, MDC algorithms do not require the use of secret information such as a cryptographic key. Such techniques are therefore highly useful in allowing encryption and message authentication to be implemented in different protocol layers in a **communication** system **without** key management difficulties, as well as in implementing **digital signature** schemes. It is shown that cryptographic checksums that are intended to detect fraudulent messages should be of the order of 128 bits in length, and the ANSI X9.9-1986 message authentication standard is criticized on that basis. A revised 128-bit MDC algorithm is presented which overcomes the so-called triple birthday attack introduced by Coppersmith. A fast, efficient implementation is discussed which makes use of the Intel 8087/80287 numeric data processor coprocessor chip for the IBM PC/XT/AT and

similar microcomputers. (6 Refs)
Subfile: B C
Descriptors: codes; cryptography
Identifiers: accidental modifications; high speed manipulation detection ; IEC; checksum algorithms; malicious modifications; electronic message ; ; ment; encryption; message authentication; protocol layers; **digital signature** schemes; triple birthday attack; Intel 8087/80287; numeric data processor coprocessor chip
Class Codes: B6120B (Codes); C1260 (Information theory); C6130 (Data handling techniques)

7/5/7 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

01696796 INSPEC Abstract Number: C81018505
Title: Application of digital signatures **based on public key cryptosystems**
Author(s): Davies, D.W.; Price, W.L.
Issued by: Nat. Phys. Lab., Teddington, UK
Publication Date: Dec. 1980 Country of Publication: UK 32 pp.
Report Number: NPL-DNACS-39/80
Language: English Document Type: Report (RP)
Treatment: Applications (A)
Abstract: In order to use fully the communication features of the 'office of the future' it will be necessary to authenticate documents in the way that a signature does, but even more securely. Several schemes for **digital signatures** have been published. The authors concentrate on true signatures based on public key cryptosystems such as that of Rivest, Shamir and Adleman (1978). Methods are proposed for signing documents of any length with a **separate signature** that can be **sent separately** , in principle, whether the document is enciphered or not. One method uses the DES cipher to form a 'digest' of the document for signature. The other uses the same kind of calculation as the RSA cipher and is therefore most useful when RSA hardware is available. The methods proposed have been devised to resist a number of types of forgery which defeat the more obvious schemes. Further criticism of the methods is welcomed. The authors continue with a discussion of the public organisation needed to support the widespread use of these signatures-a registry of public keys and a signature certification service. (8 Refs)
Subfile: C
Descriptors: cryptography
Identifiers: **digital signatures** ; true signatures; public key cryptosystems; DES cipher; RSA cipher; signature certification service
Class Codes: C0230 (Economic, social and political aspects); C6130 (Data handling techniques)

7/5/8 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus
(c)2004 Japan Science and Tech Corp(JST). All rts. reserv.

01995983 JICST ACCESSION NUMBER: 94A0178539 FILE SEGMENT: JICST-E
Cryptography and Information Security. Subliminal Channels for Transferring Signatures: Yet Another Cryptographic Primitive.
[illegible]AI K (1); ITOH T (2)
(1) Mitsubishi Electric Corp., Kamakura-shi, JPN; (2) Tokyo Inst. Technology, Yokohama-shi, JPN
IEICE Trans Fundam Electron Commun Comput Sci(Inst Electron Inf Commun Eng) , 1994, VOL.E77-A,NO.1, PAGE.31-38, REF.47
JOURNAL NUMBER: F0699CAT ISSN NO: 0916-8508
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3
LANGUAGE: English COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: This paper considers the subliminal channel, hidden in an

identification scheme, for transferring signatures. We observe the direct parallelization of the Fiat-Shamir identification scheme has a subliminal channel for the transmission of the **digital signature** . A positive aspect of this hidden channel supplies us how to **transfer signatures without** secure channels. As a formulation of such application, we introduce a new notion called privately recordable signature. The privately recordable signature is generated in an interactive protocol between a signer and a verifier, and only the verifier can keep the signatures although no third adversary can record the signatures. In this scheme, then the disclosure of the verifier's private coin turns the signer's signature into the ordinary **digital signature** which is verified by anybody with the singer's public key. The basic idea of our construction suggests the novel primitive that a **transferring** securely **signatures without** secret channels could be constructed using only one-way function (**without** trapdoor). (author abst.)

8/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

05073325 E.I. No: EIP98074302582
Title: Threshold signature schemes with traceable signers in group communications
Author: Wang, Ching-Te; Lin, Chu-Hsing; Chang, Chin-Chen
Corporate Source: Natl Chung Cheng Univ, Chiayi, Taiwan
Source: Computer Communications v 21 n 8 Jun 25 1998. p 771-776
Publication Year: 1998
CODEN: COCOD7 ISSN: 0140-3664
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9809W4
Abstract: We propose a new group-oriented (t,n) threshold signature scheme that can withstand conspiracy attacks without attaching a secret number. The group's public key is determined by all members, each member signs a message **independently** and **transmits** the individual **signature** to a designated clerk who checks and integrates them into a group signature. A verifier can authenticate the group signature and trace back to find the signers. Further, we develop another threshold signature scheme without a trusted center. The proposed schemes possess all of the characteristics listed in Harn's scheme and are more difficult to break. (Author abstract) 18 Refs.
Descriptors: *Data communication systems; Cryptography; Security of data
Identifiers: Threshold signature schemes; Group oriented cryptography
Classification Codes:
723.2 (Data Processing)
[illegible] (Computer Software)
[illegible] COMPUTERS & DATA PROCESSING)

8/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

04525570 E.I. No: EIP96103363226
Title: Declustering of key-based partitioned signature files
Author: Ciaccia, Paolo; Tiberio, Paolo; Zezula, Pavel
Corporate Source: Univ of Bologna, Bologna, Italy
Source: ACM Transactions on Database Systems v 21 n 3 Sep 1996. p 295-338
Publication Year: 1996
CODEN: ATDSD3 ISSN: 0362-5915
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications); X; (Experimental)
Journal Announcement: 9612W2
Abstract: Access methods based on signature files can largely benefit from possibilities offered by parallel environments. To this end, an effective declustering strategy that would **distribute signatures** over a set of parallel **independent** disks has to be combined with a synergic clustering which is employed to avoid searching the whole signature file when executing a query. This article proposes two parallel signature file organizations, Hamming Filter (HF) and Hamming** plus Filter (H** plus F), [illegible] common declustering strategy is based on error correcting codes, and [illegible] clustering is achieved by organizing signatures into fixed-size [illegible]s, each containing signatures sharing the same key value. HF allocates signatures on disks in a static way and works well if a correct relationship holds between the parameters of the code and the size of the file. H** plus F is a generalization of HF suitable to manage highly dynamic files. It uses a dynamic declustering, obtained through a sequence of codes, and organizes a smooth migration of signatures between disks so that high performance levels are retained regardless of current file size. Theoretical analysis characterizes the best-case, expected, and worst-case behaviors of these organizations. Analytical results are verified by experiments on prototype systems. (Author abstract) 27 Refs.
Descriptors: *Parallel processing systems; File organization; Error

correction; Codes (symbol[redacted] Software prototyping; Information retrieval; Database systems; Performance
Identifiers: Parallel environments; Superimposed coding; Organizing signatures; Error correcting codes; Parallel independent disk; Partial match queries; Prototype systems
Classification Codes:
722.4 (Digital Computers & Systems); 723.2 (Data Processing); 721.1 (Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory); 723.1 (Computer Programming); 903.3 (Information Retrieval & Use); 723.3 (Database Systems)
722 (Computer Hardware); 723 (Computer Software); 721 (Computer Circuits & Logic Elements); 903 (Information Science)
72 (COMPUTERS & DATA PROCESSING); 90 (GENERAL ENGINEERING)

8/5/15 **(Item 1 from file: 35)**
DIALOG(R)File 35:Dissertation Abs Online

01808069 ORDER NO: AADAA-I9938804
Diversity, decoding, and signal design for multiuser communications
Author: Fain, Eric Andrew
Degree: Ph.D.
Year: 1999
Corporate Source/Institution: University of Colorado at Boulder (0051)
Director: Mahesh K. Varanasi
Source: VOLUME 60/07-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 3450. 210 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL
Descriptor Codes: 0544
ISBN: 0-599-40057-9

Correlated-waveform multiple-access (CWMA) is a multiuser signaling scheme for mobile/cellular wireless communications which encompasses TDMA, FDMA, and CDMA (code-division multiple-access). A CWMA system is one in which each independent user modulates a signature waveform, and these waveforms are generally correlated with each other.

We present a generalized fading diversity model for CWMA channels, which unifies several previous approaches to diversity. Performance bounds are derived for the pre-combining group detector, which operates on the CWMA diversity channel. A new measure for analyzing such systems, the interasymptotic SNR gap, is also presented. The Group Metric Decoder, a new reduced-complexity decoder, is developed for jointly detecting and decoding users over the CWMA diversity channel. This decoder operates by assuming knowledge of only a subset of the users' codes. Performance bounds for this decoder are derived, and a new technique for bounding bit-error probabilities for fading channels is presented.

In order to analytically characterize the frequency content of CWMA and other types of signals, we introduce a new class of generalized bandwidth measures, of which RMS bandwidth and fractional out-of-band power are special cases. These measures are defined in terms of a frequency weighting function. The key feature of such measures is their relation to a special eigenvalue/eigenfunction equation which generates an associated minimum-bandwidth signal basis.

Using this minimum-bandwidth basis, we present new results for bandwidth-constrained CWMA **signature** waveform design. First, we characterize signal sets whose bandwidth is **independent** of the received power **distribution** . Such **signature** waveforms have a “location-invariant” bandwidth. Restricting attention to this class of waveforms, we present signal design procedures which maximize channel capacity under generalized bandwidth constraints. Coded and uncoded performance is maximized for signals which are, in general, correlated. Further, because of the construction of the generalized bandwidth measures, all of the signal design procedures optimized for one bandwidth measure can be easily reworked for another bandwidth measure in the class.

8/5/23 **(Item 7 from file: 2)**

DIALOG(R)File 2:INSPEC

4753504 INSPEC Abstract Number: C9410-6130S-032
Title: A survey of information authentication techniques
Author(s): Smuts, W.B.
Author Affiliation: Dept. of Comput. Sci., UNISA, Pretoria, South Africa
Journal: South African Computer Journal no.11 p.84-90
Publication Date: May 1994 Country of Publication: South Africa
CODEN: SACJE3 ISSN: 1015-7999
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Electronic documentation and the communication of these documents have become an integral part of our society. The ease with which these documents can be generated, copied, changed and communicated forms the main reason for its success. Sadly, these same attributes also form its Achilles heel. Electronic documents are so easy to generate, copy, change and **communicate** , that the authenticity of such documents is at stake. The written **signature** provides the necessary authentication in the case of paper documents. **Without** an electronic counterpart for the written **signature** , the electronic documentation and **communication** system may collapse as fast as it has grown. This article provides a survey of message authentication techniques which can be used to authenticate electronic information. It focuses on the use of public key ciphers to implement an authentication scheme. (19 Refs)
Subfile: C
Descriptors: message authentication; public key cryptography
Identifiers: electronic documents; survey; information authentication techniques; written signature; message authentication techniques; public key ciphers
Class Codes: C6130S (Data security); C0230 (Economic, social and political aspects)

8/5/24 **(Item 8 from file: 2)**
DIALOG(R)File 2:INSPEC

4566498 INSPEC Abstract Number: B9402-6120B-063, C9402-6130S-033
Title: Two efficient server-aided secret computation protocols based on the addition sequence
Author(s): Chi-Sung Laih; Sung-Ming Yen; Lein Harn
Author Affiliation: Dept. of Electr. Eng., Nat. Cheng Kung Univ., Tainan, Taiwan
Conference Title: Advances in Cryptology - ASIACRYPT '91. International Conference on the Theory and Application of Cryptology Proceedings p. 450-9
Editor(s): Imai, H.; Rivest, R.L.; Matsumoto, T.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1993 Country of Publication: West Germany x+498 pp.
ISBN: 3 540 57332 1
Conference Sponsor: Int. Assoc. Cryptologic Rec.; Inst. Electron. Inf. & Common. Engineers
Conference Date: 11-14 Nov. 1991 Conference Location: Fujiyoshida, Japan
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: A server-aided secret computation protocol (SASC) is a method that allows a client (e.g. smart card) to compute a function efficiently with the aid of a powerful server (e.g. compute) without revealing the client's secrets to the server. T. Matsumoto et al. (1988) proposed a solution to the problem which is suitable for the RSA cryptosystem. S. Kawamura et al. (1989) have shown that a client with a 10/sup 5/ times more powerful server's aid, can compute an RSA **signature** 50 times faster than the case **without** a server if the **communication** cost can be ignored. The authors propose two SASC protocols based on the addition sequence to improve the efficiency. In the first protocol, since the addition sequence is determined by the server, it can improve the computational efficiency of

the server only and it is suitable for the low speed communication link (e.g. 9.6 Kbps). It is expected that a client, with a 8982 times more powerful server's aid, can compute an RSA signature 50 times faster than the case without a server. In the second protocol, since the addition sequence is determined by the client, it can improve the computational efficiency of the client and sever simultaneously but takes more communication time and it is suitable for the high speed communication link (e.g. above 10 Mbps). It is expected that a client, with a 3760 times more powerful server's aid, can compute an RSA signature 200 times faster than the case without a server. (11 Refs)
Subfile: B C
Descriptors: cryptography; protocols
Identifiers: server-aided secret computation protocols; addition sequence ; smart card; computational efficiency; low speed communication link; RSA signature; communication time
Class Codes: B6120B (Codes); B6150M (Protocols); C6130S (Data security); C5640 (Protocols)

8/5/43 (Item 1 from file: 434)
DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

01151519 Genuine Article#: D1615 Number of References: 1
Title: **SHOWING CREDENTIALS** WITHOUT **IDENTIFICATION** SIGNATURES TRANSFERRED **BETWEEN UNCONDITIONALLY UNLINKABLE PSEUDONYMS**
Author(s): CHAUM D
Corporate Source: CTR MATH & COMP SCI,KRUISLAAN 413/1098 SJ AMSTERDAM//NETHERLANDS/
Journal: LECTURE NOTES IN COMPUTER SCIENCE, 1986, V219, P241-244
Language: ENGLISH Document Type: ARTICLE
Geographic Location: NETHERLANDS
Cited References:
CHAUM D, 1985, V28, P1030, COMMUN ACM

8/5/48 (Item 5 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

01116722 Genuine Article#: FX556 Number of References: 13
Title: PERFORMANCE OF BINARY AND QUATERNARY DIRECT-SEQUENCE SPREAD-SPECTRUM MULTIPLE-ACCESS SYSTEMS WITH RANDOM SIGNATURE SEQUENCES
Author(s): GERANIOTIS E; GHAFFARI B
Corporate Source: UNIV MARYLAND,DEPT ELECT ENGN/COLLEGE PK//MD/20742; UNIV MARYLAND,SYST RES CTR/COLLEGE PK//MD/20742
Journal: IEEE TRANSACTIONS ON COMMUNICATIONS, 1991, V39, N5, P713-724
Language: ENGLISH Document Type: ARTICLE
Geographic Location: USA
Subfile: SciSearch; CC ENGI--Current Contents, Engineering, Technology & Applied Sciences
Journal Subject Category: ENGINEERING, ELECTRICAL & ELECTRONIC; TELECOMMUNICATIONS
Abstract: The performance of synchronous and asynchronous, binary and quaternary (with and **without** offset) direct-sequence spread-spectrum multiple-access **communication** systems employing random **signature** sequences and arbitrary chip waveforms is investigated. The average probability of error at the output of the correlation receiver is evaluated using a characteristic-function approach for all the above systems. Numerical results are presented that illustrate performance comparisons between systems employing random and deterministic signature sequences, synchronous and asynchronous systems, systems with rectangular or sinewave chip waveforms, and binary quaternary systems with the same data rates and bandwidth. In all cases, the accuracy of the Gaussian approximation is also examined.
Identifiers--KeyWords Plus: CHANNELS
Cited References:
GERANIOTIS E, 1990, V8, P489, IEEE J SEL AREA COMM

GERANIOTIS E, 1986, V P756, IEEE T COMMUN
GERANIOTIS EA, 1985, V3, P695, IEEE J SEL AREA COMM
GERANIOTIS EA, 1982, V30, P985, IEEE T COMMUN
GERANIOTIS EA, 1984, P148, 1984 P C INF SCI SYS
LEHNERT JS, 1987, V35, P87, IEEE T COMMUN
POOR HV, 1988, V36, P50, IEEE T COMMUN
PURSLEY MB, 1981, P139, AUG IEEE T COMM
PURSLEY MB, 1977, V25, P795, IEEE T COM
PURSLEY MB, 1979, V27, P1597, IEEE T COMMUN
PURSLEY MB, 1980, V1, JUN IEEE INT C COMM
PURSLEY MB, 1981, P139, MULTIUSER COMMUNICAT
ROEFS HFA, 1977, R785 U ILL CHAMP COO

8/5/49 (Item 1 from file: 99)

1550071 H.W. WILSON RECORD NUMBER: BAST97046493

Recursive hashing functions for n-grams

Cohen, Jonathan D;

ACM Transactions on Information Systems v. 15 (July '97) p. 291-320
DOCUMENT TYPE: Feature Article ISSN: 1046-8188 LANGUAGE: English
RECORD STATUS: Corrected or revised record

ABSTRACT: Methods for the rapid hashing of consecutive n-grams, using a recursive hash function, are discussed. The power-of-2 integer division method was found to give the best mean uniformity, while the integer division methods are the most erratic in distribution, often producing the flattest distributions, but occasionally producing the poorest ones. Polynomial division is more general and is more suited to longer n-grams than hashing by cyclic polynomials, but the use of cyclic polynomials holds a slight edge in uniformity and in speed. Of the 4 methods outlined, recursive hashing by polynomial division or cyclic polynomials provides the most rapid processing, **without** sacrificing near-ideal **hash** value **distribution** .

File 275:Gale Group Comput[redacted] DB(TM) 1983-2004/Feb 11
(c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Feb 11
(c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Feb 11
(c) 2004 The Gale Group
File 16:Gale Group PROMT(R) 1990-2004/Feb 11
(c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2004/Feb 11
(c)2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/Feb 10
(c) 2004 McGraw-Hill Co. Inc
File 15:ABI/Inform(R) 1971-2004/Feb 10
(c) 2004 ProQuest Info&Learning
File 647:CMP Computer Fulltext 1988-2004/Feb W1
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Feb W1
(c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Feb 10
(c) 2004 The Dialog Corp.
File 369:New Scientist 1994-2004/Feb W1
(c) 2004 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc

Set	Items	Description
S1	472675	SIGNATURE? ? OR HASH?? OR DIGEST? ?
S2	3700295	SEPARATE OR SEPARATELY OR INDEPENDENT? OR DETACHED OR UNATTACHED OR (DE OR UN)()ATTACHED OR DISCONNECTED OR ISOLATED OR APART()"FROM"
S3	3888283	WITHOUT OR BY()ITSELF OR ("NOT" OR T)(1W)(INCLUD? OR ATTACH? OR WITH OR CONNECT? OR DEPENDENT?)
S4	506	S1(5N)S2:S3(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSION OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BROADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COMMUNICAT? OR FORWARD?)
S5	319	RD S4 (unique items)
S6	193	S5 NOT PD>19991112
S7	88	SIGNATURE(5N)S2(5N)(SENT??? OR SEND OR TRANSMIT? OR TRANSMISSION OR CONVEY? OR DISTRIBUT? OR TRANSFER? OR TRANSPORT? OR BROADCAST? OR DELIVER? OR DOWNLOAD? OR UPLOAD? OR STREAM? OR COMMUNICAT? OR FORWARD?)
S8	34	S6 AND S7

8/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01761331 SUPPLIER NUMBER: 16640435 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Do you know where your data is? (security measures) (Expert's Toolbox) (Column)
Lane, Alex
AI Expert, v00000010, n3, p13(2)
March, 1995
DOCUMENT TYPE: Column ISSN: 0888-3785 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1443 LINE COUNT: 00111

... the key (the truly paranoid might obtain the author's key from any number of public keyservers or from the author).
The SecureDrive **distribution** contains a set of **separate signature** files that correspond to the executables. By supplying the name of the respective signature and executable files on the command line, PGP can verify quickly...

8/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01698439 SUPPLIER NUMBER: 16219952 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Firm has technology you can bank on; with "digital cash," transactions made over public networks remain secure and private. (Tech View) (DigiCash BV's electronic cash)
Sullivan, Eamonn
PC Week, v11, n34, p83(3)
August 29, 1994
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1758 LINE COUNT: 00135

... contents of the document (typically with some kind of hash function or checksum) and then encrypts that number with his or her private key. The **signature** can be embedded in a document or **sent** in a **separate** file.
To verify that a document was signed by the sender and has not been altered since it was signed, the recipient looks up the...

8/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01611597 SUPPLIER NUMBER: 14065281 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Document signing at a distance is latest remote-work innovation. (the TeleSignature 2000 turnkey system from SDB Systems Inc.) (Product and Service News)
Telecommuting Review: the Gordon Report, v10, n7, p3(2)
July, 1993
ISSN: 8756-7431 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 729 LINE COUNT: 00055

... safeguards at every point of the process. The caller needs a password to view the document remotely; the signature and the document are encrypted before **transmission** so they cannot be intercepted or reproduced; each **signature** must be created and **transmitted separately**, so one remote **signature** can't be used to sign more than one document.
This system will let anyone sign a document remotely as long as they can establish...

8/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01402043 SUPPLIER NUMBER: 11322653
An a priori approach to the evaluation of signature analysis efficiency.
Caspi, P.; Piotrowski, J.; Velazco, R.
IEEE Transactions on Computers, v40, n9, p1068(4)
Sept, 1991
ISSN: 0018-9340 LANGUAGE: ENGLISH RECORD TYPE: ABSTRACT

...ABSTRACT: compresses test results when testing complex devices but has a probability of aliasing errors that are characteristic of linear feedback shift registers (LFSR). An evaluation **independent** of error **distribution** dependency in the analyzed sequence does not prohibit **signature** analysis use but benefits by using larger than usual LFSRs, such as length 32. The technique behind the evaluation is called a priori randomization and...

8/3,K/5 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

02159601 Supplier Number: 55608748 (USE FORMAT 7 FOR FULLTEXT)
Stan Lee Media Announces Trendsetting Lifestyle Brand and E-Retail Alliances.
PR Newswire, p8522
August 31, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 841

... distributes product to the department, gift, specialty and mass markets both in the United States and Canada through a network of both in-house and **independent** representatives and **distributors** . **Signature** Group is based in Minneapolis with offices in LA and manufacturing worldwide including Hong Kong, Dominican Republic and Los Angeles. They can be found at...

8/3,K/6 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

01887610 Supplier Number: 54762549 (USE FORMAT 7 FOR FULLTEXT)
EarthLink Selects Marimba's Castanet to Improve Customer Service for Its More Than One Million Members.
Business Wire, p0373
June 1, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 859

... Castanet to distribute, update, and manage its Internet access software based upon Castanet's built-in security features, bandwidth efficiency, scalability, personalization, and support for **disconnected** ...

" **Distributing** our **signature** service over the Internet presented a new set of challenges which Castanet helped us to solve. It has an extremely robust architecture that is very...

8/3,K/7 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

01808014 Supplier Number: 53874445 (USE FORMAT 7 FOR FULLTEXT)
Media Arts Group, Inc. Presents at Cruttenden Roth Growth Stock Conference.
PR Newswire, p4024
Feb 12, 1999
Language: English Record Type: Fulltext

Document Type: Newswire; Trade
Word Count: 399

... strategic relationships with such industry leaders as La-Z-Boy, Kincaid Furniture, QVC, Warner Books, Hallmark and Avon.

Raasch also described the Company's branded **distribution** strategy, which consists of Company-owned Thomas Kinkade stores, **independently** owned **Signature** Galleries, showcase dealers and wholesale dealers. The 30 Thomas Kinkade Stores and 162 Signature Galleries sell Thomas Kinkade products exclusively, while more than 2,500...

8/3,K/8 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01176738 Supplier Number: 42453253 (USE FORMAT 7 FOR FULLTEXT)
IC CARDS ALLOW INDEPENDENTS TO PRODUCE SOFTWARE FOR WIZARD (R)
News Release, p1
[illegible], 1991
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 583

... of the OZ-7000 and OZ-8000 Wizard series. The new cards are designed to use the full size screen of the OZ-8000/8200 **Signature** Series Wizards.

"Opening up the Wizard serial **communication** architecture to **independents** and providing EPROM and BASIC IC cards will turn an already accomplished business tool into a customized pocket product, with a customizable keyboard," says John...

8/3,K/9 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01028560 Supplier Number: 39901139 (USE FORMAT 7 FOR FULLTEXT)
Lundy-Farrington launches verification system for instant at-the- counter signature verification
PR Newswire, pN/A
Dec 1, 1986
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 341

... it through the FMS-300's electronics module. The captured signature is displayed immediately on the screen for checking, and after acceptance, the FMS-300 **transfers** the **signature** directly into the user's central computer system. **Separate** photographic and **signature** file storage equipment are eliminated, and FMS requires no additional branch controller devices.

FMS-300 intergrates with the other systems in Lundy-Farrington's FMS ...

8/3,K/10 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04188304 Supplier Number: 54790011 (USE FORMAT 7 FOR FULLTEXT)
MARIMBA: EarthLink selects Marimba's Castanet to improve customer service for one million+ members.
M2 Presswire, pNA
June 2, 1999

Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 865

... Castanet to distribute, update, and manage its Internet access software based upon Castanet's built-in security features, bandwidth efficiency, scalability, personalisation, and support for **disconnected** use.

" **Distributing** our **signature** service over the Internet presented a new set of challenges which Castanet helped us to solve. It has an extremely robust architecture that is very...

8/3,K/11 **(Item 2 from file: 636)**
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

04059011 Supplier Number: 53933592 (USE FORMAT 7 FOR FULLTEXT)
-SONERA LAUNCHES SIM CARD-BASED DIGITAL SIGNATURE TECHNOLOGY FOR WIRELESS NETWORKS.
Telecomworldwire, pNA
Feb 22, 1999
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 95

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...and making mobile communication networks safer for confidential business to be conducted. It is expected that the technology will be available for new generation mobile **communication** networks in the future. Sonera's digital **signature** solution is **independent** of phone operators and card and telephone manufacturers.

8/3,K/12 **(Item 3 from file: 636)**
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03798199 Supplier Number: 48233318 (USE FORMAT 7 FOR FULLTEXT)
VANGUARD PLANS TO OFFER ON-LINE ACCOUNT OPENING
Financial Net News, v3, n3, pN/A
Jan 19, 1998
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 477

... process online.
Currently, Vanguard's on-line customers who want to set up another account need to request the written materials, complete the forms and **send** in a **separate** physical **signature** to the company, authorizing the new account. Under the new system, the physical signature that was filed with Vanguard to establish the original account will...

8/3,K/13 **(Item 4 from file: 636)**
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01196136 Supplier Number: 46548533 (USE FORMAT 7 FOR FULLTEXT)
CON CONGRESSDAILY Kennedy Backs Daschle Suggestion For Health Bill Split
CongressDaily/A.M., pN/A
July 16, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 333

(USE FORMAT 7 FOR FULLTEXT)

TEXT:
...during a joint appearance with Senate Majority Leader Lott on NBC's "Meet the Press", Republicans "would agree to let these insurance reforms be passed **separately** and **sent** to the president" for his presumed **signature** . Democrats then would agree to allow a vote on a **separate** bill creating tax-sheltered MSAs that Republicans have tried to include in the portability bill. "The strategy of separating the issues broke the recent Senate...

8/3,K/14 (Item 5 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

02314329 Supplier Number: 44498385 (USE FORMAT 7 FOR FULLTEXT)
BRADLEY, WALLOP ADD 45 SIGNATURES TO ANTI-ROS LETTER
Octane Week, v9, n10, pN/A
March 7, 1994
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1268

... 2/14/94, p1), the letter represents the strongest political challenge yet to the ROS.
Meanwhile, Senate Majority Leader George Mitchell (D-ME) pulled his **signature** from the letter, and Department of **Transportation** Secretary Federico clarified **separately** that he is not opposed to the ROS.
"We are writing to make clear our opposition to the EPA's proposed rule to mandate the...

8/3,K/15 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06651065 Supplier Number: 55810828 (USE FORMAT 7 FOR FULLTEXT)
Respond Plans 25th Anniv. Tour.(Statistical Data Included)
HAY, CARLA
Billboard, v111, n38, p15
Sept 18, 1999
Language: English Record Type: Fulltext
Article Type: Statistical Data Included
Document Type: Magazine/Journal; General
Word Count: 568

... songs from Boston-area female singer/songwriters, such as Juliana Hatfield, Mary Lou Lord, and Melissa Ferrick (Billboard, Jan. 23). The set was released on **independent** label **Signature** Sounds, **distributed** by Koch International.
The organization and album have since received high-profile support, including exposure via MTV, VH1, and Lilith Fair (Billboard, May 29).
"Respond...

8/3,K/16 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04775041 Supplier Number: 47028703 (USE FORMAT 7 FOR FULLTEXT)
Market Expands For Indie Folk Labels
Horak, Terri
Billboard, p1
Jan 11, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; General
Word Count: 1514

... Olsen, president/founder of Signature Sounds, a label that

specializes in musicians based around its Northhampton, Mass., home base, supports the pooling of resources for **independents** within the special-interest group.

Signature Sounds signed a **distribution** deal with Koch International in September 1996 and has just released its first sampler, which will be included in the February issue of roots music...

8/3,K/17 **(Item 3 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

04578606 Supplier Number: 46731045
Motorola goes for the hard cell.
Business Week, p39
Sept 23, 1996
Language: English Record Type: Abstract
Document Type: Magazine/Journal; General Trade

ABSTRACT:
Motorola Inc.'s plan to increase cellular phone sales by limiting distribution of high-end cellular phones has angered many **distributors**. The plan, dubbed the **Signature** program, stipulates that cellular carriers and **independent** retailers meet certain conditions, in return for selling Motorola's $1,300 StarTAC phone loaded with high-end features. Motorola requires that distributors must put...

8/3,K/18 **(Item 4 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

04137058 Supplier Number: 46037680 (USE FORMAT 7 FOR FULLTEXT)
Congress kills ICC after last-minute haggling
Traffic World, p10
Jan 1, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 623

... Dec. 21 and the House on Dec. 22 gave final approval to the ICC Sunset Act of 1995, sending it to President Clinton for his **signature**.

The legislation creates a new **independent** Surface **Transportation** Board within the Department of Transportation that will handle those railroad and motor carrier functions not repealed by Congress. DOT will assume jurisdiction over the...

8/3,K/19 **(Item 5 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

03821943 Supplier Number: 45458442 (USE FORMAT 7 FOR FULLTEXT)
Lacroix Banking on Bazar, Jeans
WWD, v0, n0, p14
April 6, 1995
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 901

... great opportunity. We believe that his jeans line can be very important,' Gerani said.

A key element in Bensoussan's recovery strategy has been to **separate** the creation and **distribution** of Lacroix's different apparel collections.

The **signature** line is licensed to Mendes, the top-quality apparel maker that also manufactures Yves Saint Laurent's Rive Gauche. Bazar is sourced from the Loire...

8/3,K/20 **(Item 6 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

02708512 Supplier Number: 43619333 (USE FORMAT 7 FOR FULLTEXT)
Apparel
Golf Pro Merchandiser, p31
Feb, 1993
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 3660

... custom-designed shirts with hole-designs printed across the front.
YEAR ENTERED GOLF BUSINESS: 1991
PRODUCT CATEGORIES: Apparel
NEW FOR 1993: Shirts for clubs with **signature** hole printed on shirt
SALES REPS: 12 **independent**
DISTRIBUTION : On- and off-course
TERMS: Net 30
ADVERTISING CAMPAIGN: Golf Pro Merchandiser, Golf Shop Operations, Sarasota Magazine
ADVERTISING THEME: 'Style has no handicap.'
SPECIAL PROMOTIONS...

8/3,K/21 **(Item 7 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

01463179 Supplier Number: 41658538 (USE FORMAT 7 FOR FULLTEXT)
TV violence bill addressed
Video Week, pN/A
Nov 5, 1990
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 278

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
Jury remains out on how broadcasters will approach TV violence bill (S-593) that at week's end was awaiting President Bush's **signature** , Assn. of **Independent** TV Stations (INTV) and National Assn. of **Broadcasters** (NAB) said. Bill would give broadcast, cable and film industries temporary waiver of antitrust laws to develop voluntary program guidelines. "Will the television industry use...

8/3,K/22 **(Item 1 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

11326220 SUPPLIER NUMBER: 55693423 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Filing for aid? Here's help. (Brief Article)
Lord, Mary; Moll, Jason
U.S. News & World Report, 127, 9, 90
Sept 6, 1999
DOCUMENT TYPE: Brief Article ISSN: 0041-5537 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1064 LINE COUNT: 00084

... 104).
Any parent or preparer who supplied information must sign the form, or it will be returned unprocessed. Those filling out an online FAFSA must **send** in a **separate signature** page; this attests to the form's accuracy and allows schools to receive your report. Save a copy of your application and work sheets, which...

8/3,K/23 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09235855 SUPPLIER NUMBER: 18993255 (USE FORMAT 7 OR 9 FOR FULL TEXT)
2nd-generation executive leads reborn WTBS. (WTBS-TV President William Burke)
Broadcasting & Cable, v126, n52, p117(1)
Dec 16, 1996
ISSN: 1068-6827 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 801 LINE COUNT: 00064

Burke, who was 10 years old when TBS started in 1976, will be responsible for developing the network's **signature broadcasting** as the nation's top **independent** station.

Given his family roots, it was an all but foregone conclusion that Burke would someday work in the broadcast business. His father, Daniel Burke...

8/3,K/24 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

07812130 SUPPLIER NUMBER: 16792562 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lacroix banking on Bazar, jeans.(Christian Lacroix S.A.)
Deeny, Godfrey
WWD, v169, n66, p14(2)
April 6, 1995
ISSN: 0149-5380 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 944 LINE COUNT: 00071

... great opportunity. We believe that his jeans line can be very important," Gerani said.

A key element in Bensoussan's recovery strategy has been to **separate** the creation and **distribution** of Lacroix's different apparel collections.

The **signature** line is licensed to Mendes, the top-quality apparel maker that also manufactures Yves Saint Laurent's Rive Gauche. Bazar is sourced from the Loire...

8/3,K/25 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

06459456 SUPPLIER NUMBER: 13626950 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Plugged-in taxpayers are filing state, federal returns together. (Internal Revenue Service encouraging electronic filing)
Quindlen, Terrey Hatcher
Government Computer News, v12, n8, p1(2)
April 12, 1993
ISSN: 0738-4300 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 721 LINE COUNT: 00057

... Monaco said. "We just allow it to come in as a piggyback."

State officials then pull the information from the directory for their state. The **transmitter** of the tax returns sends **separate signature** documents to the IRS and the state.

FedState saves the states money and time, Idziak said. "The IRS basically acts as a post office," she...

8/3,K/26 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

06222826 SUPPLIER NUMBER: 14176801 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Hospitals, chapters weather Hurricane Andrew. (Healthcare Financial Management Association, Florida chapter) (Provider Perspective) (Column)
Siwicki, Bill
Healthcare Financial Management, v46, n11, p72(2)
Nov, 1992
DOCUMENT TYPE: Column ISSN: 0735-0732 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1181 LINE COUNT: 00095

... see that out of this terrible tragedy comes something good--people helping each other."
HFMA National staff has supported Broadway and the Disaster Fund by **distributing** two **separate** fund-raising letters.
The first letter bore Broadway's **signature** and was sent to the entire HFMA Florida membership. HFMA National staff volunteers had the document printed, stuffed the envelopes, and mailed the letters.
The...

8/3,K/27 **(Item 6 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

03900038 SUPPLIER NUMBER: 06967948 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Second Annual Directory of Human Resources Services, Products and Suppliers, January 1989. (directory)
Personnel, v66, n1, pD1(167)
Jan, 1989
DOCUMENT TYPE: directory ISSN: 0031-5702 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 155534 LINE COUNT: 14711

8/3,K/28 **(Item 7 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

03154879 SUPPLIER NUMBER: 04770616 (USE FORMAT 7 OR 9 FOR FULL TEXT)
National Conference of Catholic Bishops-United States Catholic Conference issues information and application for selected members of the news media who wish to accompany Pope John Paul II on his United States visit in September.
PR Newswire, FL5
April 21, 1987
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 727 LINE COUNT: 00070

... Name of Immediate Supervisor: ---------- Have you applied to Archdiocese of Miami for basic press credential? --------- IS 50 PERCENT NON-REFUNDABLE DEPOSIT:
A. ( ) Included
or
B. ( ) **Sent** under **separate** cover

Signature of Applicant
---------- For Office Use Only
/PRNewswire -- April 21/

8/3,K/29 **(Item 8 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

02479289 SUPPLIER NUMBER: 03920097 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Eluding the enemy: ECCM techniques; electronically foiling the enemy's communications interception can turn the tide of combat.
Amoroso, Frank

...Electronics, v17, p171(11)
..., 1991
ISSN: 0278-3479 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 5959 LINE COUNT: 00475

... as quadriphase shift keying, do not yield periodic components on being squared, but rather cause an expansion of bandwidth. Therefore, they may be preferred for **signature** intercept-resistant **transmission** .

A somewhat **independent** approach to LPI has sprung up around the phenomenon of oxygen absorption of electromagnetic energy in the atmosphere. Atmospheric gases, including water vapor, absorb radiation...

8/3,K/30 **(Item 1 from file: 15)**
DIALOG(R)File 15:ABI/Inform(R)

01825161 04-76152
Trust in information management: Bank turns to common database solution for vital functions
Silver, Judy
Inform v13n5 PP: 34-35 May 1999
ISSN: 0892-3876 JRNL CODE: IFN
WORD COUNT: 1432

...TEXT: to take advantage of Windows, distributed processing, relational database, and install a Y2K application," said Jacques. "Lastly, we wanted to change our method of archiving, **distributing** , and viewing **signature** cards from microfiche to imaging."

After conducting an **independent** evaluation of document imaging systems that met the necessary criteria, St. Johns selected OnBase Information Management System, from Hyland Software Inc. "The single most important...

8/3,K/31 **(Item 2 from file: 15)**
DIALOG(R)File 15:ABI/Inform(R)

01284322 99-33718
Public key mystery
Kerr, Deborah
Computerworld v30n37 PP: 93-94 Sep 9, 1996
ISSN: 0010-4841 JRNL CODE: COW
WORD COUNT: 1670

...TEXT: verify the sender's authenticity. It's loosely based on complex mathematical factoring.

Over at Berkeley in 1975, Merkle had formed the problem of secure **communication** **independent** of **signature** and certificate. He was attacking the **distribution** of the public key based on random numeric puzzles as his premise. When he read the Hellman-Diffie paper, Merkle looked up Hellman, who talked...

8/3,K/32 **(Item 3 from file: 15)**
DIALOG(R)File 15:ABI/Inform(R)

00967129 96-16522
What does it all mean?
Spaeth, Tony
Across the Board v32n2 PP: 53-55 Feb 1995
ISSN: 0147-1554 JRNL CODE: CBR
WORD COUNT: 2021

...TEXT: the bet, Landor proposed another unorthodox idea--a new "X," kind

of a second corporate lo[redacted] for promotional/marketing uses. It will "float" in Xerox **communications** , **separate** for the time being from the principal **signature** --the identity equivalent of an employee on trial.

I AM NOT SURE whether to credit Sanford I. Weill for lowest-cost identity programs (he buys...

8/3,K/33 **(Item 1 from file: 810)**
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0867016 BW1276

PRINCETON SOFTECH: Princeton Softech Executive Addresses Y2K Symposium At Major Telecommunications Company

June 16, 1998

Byline: Business Editors

...worldwide. It provides clients with resource augmentation and advanced technology solutions to business problems, including its industry-leading solution to the millennium date-change problem, **Signature** 2000(tm). Through **independent distributors** , products are also available in Europe, Australia, Latin America, Asia, Africa, and the Middle East.

CONTACT: Princeton Softech, Inc.
David Craig, Joe Allegra
(800) 457...

8/3,K/34 **(Item 2 from file: 810)**
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0835282 BW1607

COMPUTER HORIZONS: Year 2000 Wire/Computer Horizons, Mercury Interactive Leverage Strengths to Improve Year 2000 Testing

April 14, 1998

Byline: Business/Technology Editors

...worldwide. It provides clients with resource augmentation and advanced technology solutions to business problems, including its industry-leading solution to the millennium date-change problem, **Signature** 2000. Through **independent distributors** , products are also available in Europe, Australia, Latin America, Asia, Africa, and the Middle East. E-mail address for more information is: information@chc.fabrik...